



SECURE DYNAMIC CLOUD FOR
INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY
BASED ON PAN-EUROPEAN DISASTER INVENTORY

Deliverable 2.7

**ELSI Guidance for 21st Century
Networked Crisis Management**

Final

Katrina Petersen and Monika Büscher (Editors)

ULANC

April 2017

Work Package 2

Project Coordinator

Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme
for Research and Technological Development

COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems
and data set used by first responders and police authorities





Distribution level		Public		
Due date		30/04/2017		
Sent to coordinator		27/04/2017		
No. of document		D2.7		
Name		ELSI Guidelines for 21st Century Networked Crisis Management		
Type		Public		
Status & Version		1.0		
No. of pages		77		
Work package		2		
Responsible		ULANC		
Further contributors		BAPCO, KEMEA, UPB		
Authors		Katrina Petersen, Monika Büscher, Xaroula Kerasidou, Sarah Becklake, Catherine Easton, Malé Luján Escalante, Paul Hirst, Christina Schaefer		
Keywords		ELSI, Key Terms, Guidance, EIA, PIA, Reflexivity, Collaboration, Disaster, Information Technology, CIS		
History	Version	Date	Author	Comment
	V0.1	01/03/2015	Petersen	First Draft Structure
	V0.2	20/03/2016	Petersen	Updated chapter list
	V1.0	05/04/2017	Petersen, Kerasidou, Escalante	Büscher, Easton, Version for QA review
	V1.1	13/04/2017	Christina Schaefer	QA review
	V1.2	22/04/2017	Ioannis Daniilidis	QA review
	V2.0	27/04/2017	Petersen	Final Version for Submission

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.



Authors



University of Paderborn
C.I.K.

Christina Schäfer
Email: c.schaefer@cik.upb.de



Centre for Mobilities Research
Department of Sociology
Lancaster University
LA1 4YD
UK

Monika Büscher
Email: m.buscher@lancaster.ac.uk
Katrina Petersen
Email: k.petersen@lancaster.ac.uk
Sarah Becklake
Email: s.becklake@lancaster.ac.uk
Xaroula Kerasidou
Email: x.kerasidou@lancaster.ac.uk
Malé Luján Escalante
Email: m.lujanescalante@lancaster.ac.uk
Catherine Easton
Email: c.easton@lancaster.ac.uk



Airbus Defence and Space

Olivier Paterour
Email: Olivier.Paterour@airbus.com



British APCO

Paul Hirst
Email: paul.hirst@bapco.org.uk



Reviewers



University of Paderborn
C.I.K.

Christina Schäfer
Email: c.schaefer@cik.upb.de



Center for Security Studies
(KEMEA)
P.Kanellopoulou 4
1101 77 Athens
Greece

Ioannis Daniilidis
Email: i.daniilidis@kemea-research.gr



Executive summary

This deliverable has four goals:

- 1) Outline the concept of ELSI Guidance for 21st Century networked disaster risk management (DRM);
- 2) Provide an overview of ELSI Key Terms and Guidance developed around hosting, implementation, and managing Common Information Spaces (CIS);
- 3) Explain the community platform approach for interactive engagement of stakeholders in developing the ELSI Guidance;
- 4) Explore wider societal implications of the ELSI guidance.

The introduction (Chapter 2) sets the stage for why ELSI Guidance is necessary. It argues that while many different codes of ethics exist, most treat ELSI abstractly or are only relevant to individual organisations. However, what ELSI mean and how they create challenges or (unforeseen) opportunities changes depending on the actors, technologies, goals and contexts for interactions. This chapter explains how collaboration through disaster information and communication technologies (ICT) in general, and common information spaces (CIS) in particular, requires a different type of reflexive ELSI guidance that supports critical engagement.

The next chapter (3) develops the 'ELSI Guidance Concept' for hosting, managing, and governing a CIS for collaborative information sharing in DRM. The overall aim for the ELSI Guidance is to support real world practices of collaboration and sense-making in ways that critically and creatively address ELSI arising in the increasing informationalisation of DRM, and the need to work across agencies, organisational, political and cultural borders or work with new partners. The ELSI Guidance combine explanations of Key Terms complemented by Guidance entries to seed an evolving community resource. The ELSI Key Terms are derived from the SecInCoRe inventory and ethical impact assessment (EIA) process. They define, more broadly, the ELSI related to collaborative disaster IT and provide a starting set of general aspects that need to be considered. However, while these aspects help define end-goals, they do not offer clear paths of action. The Guidance entries explore a range of questions to consider to help figure out what about the principles, values, virtues and challenges captured by the Key Terms is important to consider in specific DRM collaborative ICT situations. The chapter then provides background on how these were derived and how they relate to already existing codes of ethics in DRM and IT. It also explains the motivation for making the guidance 'live, lived, and living'. As a whole, the ELSI Guidance provide resources for those engaged in collaborative, digitally augmented DRM to consider how they might pro-actively notice and address ELSI challenges, or take advantage of ELSI opportunities.

Chapter 4 explains the ELSI Key Terms. It describes the methodology used to identify ELSI Key Terms or topics from ethical, legal, and social principles, virtues, and values in the context of collaborative disaster ICT. Providing examples, this chapter establishes how the Key Terms are intended to support exploration of ELSI that arise in situations of collaboration, coordination, or cooperation supported by information technology. The fifth (5) chapter similarly describes the ELSI Guidance developed in relation to the principles, virtues, and values captured by these Key Terms to support best practices and critically thinking about challenges and opportunities.

The sixth (6) chapter explains the forms of interactive and community engagement that have been developed around the Guidance. These are a range of tools through which to both directly use the Guidance but also to learn and explore in greater depth how the guidance can be used and when they could be of value which include a community-based platform, experimental forms of Ethical Impact Assessments, and a board game. The chapter first



describes the platform, www.isITethical.eu, upon which the Key Terms and Guidance are built for public engagement. Paired with this community-based platform, the chapter describes the governance concept behind the platform and more exploratory efforts to expand and enhance the existing content. Taking up EIAs next, the chapter argues for the need to re-specify EIAs in responsible research and innovation, suggesting a more iterative, collective and creatively experimental approach to this increasingly prominent and necessary practice. It argues that EIAs need to be conducted in ways that treat the social and technical as intertwined, not separate phases or 'checks'. Finally, it describes an offline board game that has been designed based off the Guidance in order to encourage new forms of engagement with ELSI. All three are intended to inform each other.

Chapter 7 discusses how the Guidance influenced the design practice within SecInCoRe. First is an explanation of the main features of a Common Information Space upon which SecInCoRe focused. Then the chapter presents examples of the various ways in which ELSI emerged and the ELSI guidance was implemented as part of physical design, user experience, or governance documents. These examples are not intended to be comprehensive to either the SecInCoRe project nor to how the ELSI Guidance can be implemented within collaborative disaster IT. Rather, they illustrate a range of approaches and tactics for working with this Guidance, including demonstrating how ELSI can be treated as integral to innovation – as an ongoing social and technical process – rather than an external check on design decisions.

The eighth (8) chapter, 'Wider Societal Implications', explores how the Guidance could play a role in larger socio-technical transformations in risk governance and emergency management. The chapter discusses the current challenges of ELSI in IT and DRM in relation to the current debates within the framework of European values, the shift from treating democracy as a mandate for a single voice to a practice of contestation, and the way in which new publics are being noticed and heard as a result of the new media landscape. It argues that ELSI have to turn from matters of fact, accepted and taken for granted common-sense facts of life, into 'matters of concern' situated, contextual, and the result of socio-technical work. In each case, it discusses how these challenges influenced the form the Guidance took.

Chapter 9 concludes the deliverable with a description of future work in relation to the ELSI Guidance. It describes ongoing plans for developing the content further, the aim to build isitethical.eu into a research-based service for future innovation projects in DRM as well as the intention to construct an inventory of examples of best practice in design and use.



Table of contents

1	About this document	7
1.1	Purpose of this document.....	7
1.2	Validity of this document.....	7
1.3	Relation to other documents.....	7
1.4	Contribution of this document	8
1.5	Target audience	9
1.6	Glossary.....	9
1.7	List of figures	10
1.8	List of tables	11
2	Introduction.....	12
3	ELSI Guidance Concept	15
3.1	Aims of the ELSI Guidance.....	15
3.2	Background	17
3.3	Live, Lived, Living ELSI Guidance.....	19
3.4	Added Value: Stakeholder Participation and Comments	20
4	ELSI Key Terms	23
4.1	Key Terms Overview	23
4.2	Examples	23
4.2.1	<i>Accountability</i>	<i>24</i>
4.2.2	<i>Diversity.....</i>	<i>24</i>
4.2.3	<i>Equality.....</i>	<i>26</i>
4.2.4	<i>Privacy.....</i>	<i>27</i>
4.2.5	<i>Trust.....</i>	<i>28</i>
4.3	Summary	28
5	ELSI Guidance	30
5.1	ELSI Guidance Structure and Template	30
5.2	Examples	31
5.2.1	<i>Goal Diversity.....</i>	<i>32</i>
5.2.2	<i>Decision Making.....</i>	<i>34</i>
5.2.3	<i>Data Standards.....</i>	<i>37</i>
5.2.4	<i>Recognising Relevant Collaborators.....</i>	<i>40</i>
5.2.5	<i>Protecting the Rights of Data Subjects.....</i>	<i>41</i>
5.3	Summary	43
6	Community Engagement	44



6.1	Isitethical.eu.....	44
6.1.1	<i>The interactive platform</i>	44
6.1.2	<i>Governance of the Community Platform</i>	47
6.2	Playful Offline Interaction	49
6.2.1	<i>Elements of the game</i>	50
6.3	Rethinking the EIA.....	51
7	Implementation of ELSI Guidance within the SecInCoRe project	54
7.1	Considering ELSI in Common Information Spaces	54
7.2	How ELSI translated into SecInCoRe	54
7.2.1	<i>Knowledge Base/Inventory</i>	55
7.2.2	<i>Semantic Search</i>	57
7.2.3	<i>NEC/RescueRoam/Collaborative Platform</i>	61
8	Wider Societal Implications and Future Work	63
8.1	Some comments about current societal tensions affecting this guidance	63
8.1.1	<i>Revisiting European Values</i>	63
8.1.2	<i>From unity and solidarity to contested democratic engagements</i>	64
8.1.3	<i>New media and new publics</i>	65
8.1.4	<i>Implications</i>	66
9	Future Work	67
9.1	Plans	67
9.2	Memorandum of Understanding	68
9.3	ELSI Guidance Governance	69
9.4	Further Research Required	69
10	Literature Index	71



1 About this document

1.1 Purpose of this document

This document describes the ELSI Guidance produced by SecInCoRe to support reflexive and proactive engagement with the ethical, legal, and social implications of common information space (CIS) for DRM. In doing so, it draws out questions about how collaboration and interoperability in a disaster CIS influence and are influenced by specific contexts as well as how the resulting challenges and possibilities affect the use of cross-border and European CIS (T2.4).

The work presented draws on previous research within SecInCoRe related to distributed collaboration in order to evaluate the implication of both the conceptual design and socio-technical prototypes (e.g. D2.1, D2.2, D2.4, D3.4, D4.3, D4.4, D5.4). By compiling the results of analysis the mutual dependency of technology, organisational dynamics, human factors, ethical, legal, and societal issues in relation to the existing and emergent future practices of DRM, this document is intended to galvanise those involved in ICT innovation for DRM and Pan-European coordination to see how designing ICT for collaboration risk management has to consider potential unintended consequences of design decisions (T2.4).

1.2 Validity of this document

This document has drawn input from various activities, including co-design workshops, disaster exercise observation, extended interviews with response experts from a range of European countries, and literature reviews. It builds upon existing knowledge in the consortium and balances work done at local, national level, and EU levels, providing a solid background regarding collaboration and interoperability to the conceptualization required for this project.

1.3 Relation to other documents

Inputs:

- [1] Grant Agreement (no. 607832) and Annex 1. - Description of Work
- [2] Consortium Agreement
- [3] D1.2 Research Ethics (first version): Research Ethics Protocols, relevant authorisations and informed consent
- [4] D2.1 Overview of disaster events, crisis management models and stakeholders [in the form of T2.1; T2.2 input to T2.3]
- [5] D2.2 ELSI guidelines for collaborative design and database of representative emergency and disaster events in Europe' [in the form of T2.1; T2.3]
- [6] D2.3 Report on performance, goals and needs and first draft of new crisis management models and ethical, legal and social issues [in the form of T2.2, T2.3, T2.4]
- [7] D2.4 Domain Analysis: Baseline and Emergent Future Practices [in the form of T2.1 and T2.2]
- [8] D2.5 Database of representative disaster events in Europe [in the from of T2.1, T3.1, T3.4, T4.1, T4.2]
- [9] D2.6 21st Century Crisis Management [in the form of T2.2, T2.4]
- [10] D3.2 First publication of inventory results: Incl. chapters on First version of data sets [in the form of T3.1, T3.2, T3.5]
- [11] D3.3 Second publication of inventory results, including ethnography and holistic process models and statements of future evolutions [in the form of T3.1, T3.2, T3.4, T3.5]
- [12] D3.4 Final publication of inventory results [in the form of T3.1, T3.2, T3.4, T3.5]



- [13] D4.1 Requirement Report: Incl. chapters on first requirement analysis results [In the form of T4.2]
- [14] D4.2 System Views and Concept of Operations [in the form of T4.3]
- [15] D4.3 Networked enabled communication system concept and common information space [in the form of T4.1, T4.4, T4.6]
- [16] D4.4 Report on Interoperability Aspects [in the form of T4.1, T4.5]
- [17] D6.2 Status report on Standardisation [in the form of T 6.1]

Outputs:

- [18] D5.5 Evaluation and Validation Report for SecInCoRe stakeholders [in the form of T2.2-4 input to T5.1]
- [19] D6.4 Standardisation, Exploitation, and Dissemination Report [in the form of T2.1, T2.3, T2.4]
- [20] Final EU Reporting

1.4 Contribution of this document

The work documented here contributes to all four key objectives of the project in different ways (Table 1).

Objective	Contribution of work documented in D2.7
Curation of a pan-European inventory of past critical events and disasters and their consequences.	Deriving key terms from SecInCoRe ELSI inventory. Sensitising designers, users, hosts, and those in charge of governance of CISs for DRM to ethical, legal and social implications of ICT supported collaboration, highlighting opportunities and challenges for emergent crisis management practices.
Design of a secure, dynamic cloud-based knowledge base and communication system concept including the ability to use emergency information by means of a trans-European communication infrastructure.	Clarifying the implications of design and governance decisions in relation to cross-border and pan-European CISs in ways that makes it possible to be reflexive and proactive about opportunities and challenges in collaborative work practice, information politics, organizational culture, technology dependence, data protection, digital divides, social sorting.
Conceptual integration of available ICT technology into patterns of infrastructure found in first responder organisations.	Making designers, users, and hosts conscious towards the socio-technical nature of innovation, highlighting opportunities and challenges.
Evaluation and validation of all results in representative fields of application.	Defining the object of evaluation as a socio-technical configuration of technologies, practices, policy, regulatory frameworks. Establishing a human-centred, value sensitive collaborative design and responsible research and innovation methodology. Structuring and enriching formative and summative evaluation.



Table 1 Contribution to Objectives

1.5 Target audience

The analysis and guidance are meant to underpin collaborative research and innovation within the SecInCoRe team. We make this public to engage the wider scientific and practitioner communities in the debate and set this up to be an on-going, evolving, community resource. The document is mainly aimed at those implementing, hosting, governing, or conceptually designing CISs for DRM.

1.6 Glossary

Abbreviation	Expression	Explanation
CIS	Common Information Space	Temporary environments produced by people for reasoning with information. Afford secure information disclosure, withholding, negotiation, sharing, deleting, configuring awareness, collaboration.
CJEU	The Court of Justice of the European Union	
Co-design	Collaborative Design	
Collaboration		Working together without conflating one party's goals/understandings for another.
DPA	Data Protection Authority	
DRM	Disaster Risk Management	
EIA	Ethical Impact Assessment	
ELSI	Ethical, Legal, and Social Issues	
EU	European Union	
ECHR	European Convention on Human Rights	
ICT / IT	Information and Communication Technology	
IFRC	International Federation of the Red Crescent and Red Cross	
informatonalisation		the integration of ever more information into societal processes, services and practices
Interoperability		Having one party's information, technology, and practices be understandable and usable by another party.



Interpretive context		Necessary background information in order to make sense of data in a way that does not lead to misinterpretation
ISO	International Organization for Standardization	Responsible for international management standards
JESIP	Joint Emergency Services Interoperability Programme	
LTE	Long-Term Evolution (LTE)	A standard for high-speed wireless communication for mobile phones and data terminals
MOU	Memoranda of Understanding	
PPDR	Public Protection and Disaster Response	
TC	Technical Committee	
UN	United Nations	

1.7 List of figures

Figure 1 Live, lived, living ELSI Guidance	20
Figure 2 The ELSI Guidance Front Page.....	44
Figure 3 The ELSI Guidance landing page.....	45
Figure 4 Guidance menu example.....	46
Figure 5 Example Guidance.....	46
Figure 6 ELSI Key Terms landing page (excerpt).....	47
Figure 7 Specific ELSI Key Term.....	47
Figure 8 ELSI Guidance 'Contributors' Corner'.....	48
Figure 9 ELSI Guidelines Governance	48
Figure 10 The ELSI Guidance Game.....	50
Figure 11 Screenshot of past disaster case studies within the Knowledge Base, showing (centre) the ELSI that emerged.....	55
Figure 12 Screenshot of the access denied message that appears when trying to access a restricted document. The message also suggests contacting the author and visiting the ELSI Guidance for further explanation.....	56
Figure 13 Screenshot of the search filters (left hand side) and the keyword/meta-data listing (grey box) that appears with each search result	57
Figure 14 Screenshots of graph view search sequence, following the taxonomy to see interconnections: document with tags (top), click on tag to get related documents (middle), click on new document to get more tags (bottom)	59
Figure 15 Screenshot of meta-data keyword editing	60
Figure 16 Knowledge Base entry details showing meta-data and author name (right hand side, top of list) that is an email link.	61



<i>Figure 16 The QR codes that enable the self-selected communication groups within the NEC</i>	62
<i>Figure 18 A copy of the signed MOU</i>	68

1.8 List of tables

Table 1 Contribution to Objectives	9
Table 2 Existing DRM Standardisation and Guideline Efforts	17
Table 3 ICT Ethical Standardisation and Guideline Efforts.....	19
Table 4: ELSI Guidance Table of Contents for Guidance Component	30



2 Introduction

Ethical, legal, and social issues (ELSI) arising in information sharing in Disaster Risk Management (DRM) include, among others, opportunities for more richly informed emergency planning and response, development of new (public-private) partnerships, and use of citizen data in crises, as well as risks to privacy, data protection, and liabilities. It is critical to appreciate that these are not separate from practices and technologies of networked collaboration and information exchange for DRM.

Contemporary DRM increasingly involves collaboration across cultural, political, and geographical boundaries, which forces practitioners to move away from easily shared definitions and categories. Increased complexity means that moral clarity can blur (Geertz, 1973; Mantovani, 2000). If technological innovation, practice and ELSI are seen as separate from each other, and from specific contexts, those blurred zones can become problems without solutions. For example, in innovation projects, ELSI are often treated as if they are a matter of use, arising only after design, or as if they can be addressed 'by design' prior to use or by regulation of 'proper' use (Balmer et al 2016). If ELSI are isolated like this, they cannot be addressed adequately.

There is increasing recognition that information technology can be 'good' only if it is made in consideration of how it fits into wider societal concerns, values, norms, and responsibilities (e.g. FET Advisory Group 2016). This reflects growing awareness that the attention to the social and the technological need to go hand in hand. Statements that ELSI 'are relative so it is not something I can address' ignore the fact that ELSI are neither 'in' the technologies nor their use. They are distributed across the social interactions, the technical tools, the environment in which they act, and the problems to which they are being applied. ELSI therefore need to be considered in an ongoing manner and move from being treated as the responsibility of individual users or the responsibility of persons in specific social roles, such as designers, or ethics experts, to a collective, ongoing socio-technical co-responsibility.

SecInCoRe has developed a new approach to proactively address how ELSI arise from the ways in which technology is entangled with the social. This approach combines qualitative study of existing real world practices with collaborative design of technologies, experimental and playful ways of approaching ethical impact assessment, and broad-based stakeholder consultation.

This is especially important when developing technologies for collaborative disaster risks management, because there is an increasing informationalisation in this domain. Informationalisation involves the integration of ever more information into societal processes, services and practices in general, and DRM in particular. The informationalisation of DRM is a result of an increased diversity of responders called to work together in any given disaster, making it possible to share information and support collaboration amongst distributed actors (Boersma 2010). These have encouraged just-in-time logics and logistics in other domains (Lash and Urry 1994) as well as expansive data analytics (Thrift 2005; 2011).

In emergency response, informationalisation can support enhanced risk assessment, preventative measures and learning from past events, as well as increased surge capacity, data sharing, communication and collaboration between emergency responders, closer engagement with people affected by disasters, and mobilization of collective intelligence. But, as stated by Hollnagel & Woods (2005: 7):

the belief that more data or information automatically leads to better decisions is probably one of the most unfortunate mistakes of the information society.

There are many reasons for this that are linked to ELSI. First, risk analysis is not a standardised process. Within each context (place, time, incident, need, people), different



practices and considerations may be made, and their consequences cannot be known in advance. The use of digital radio in over 125 countries in the world¹ and the rise of social media (Palen, Vieweg, Sutton & Liu 2009; Letouzé, Meier, & Vinck 2013) have, for example, fundamentally changed emergency communications and public expectations of emergency response. And while new technologies, like LTE wireless high-speed data, often focus on increasing information as a solution to problems in DRM and can enable broader and more effective collaborations, they also come with new ethical, legal, and social risks that go beyond existing guidelines available at any individual agency or organisation. Exceptions from data protection may, for example, foster surveillance and social sorting and erode values of freedom and democracy.

Second, technologies are being developed and incorporated into information sharing practices so quickly that ELSI around their design and use are often left unconsidered. In other words, the informationalization of DRM is a form of "disruptive innovation", that is, innovation that transforms the social, economic, political, and organizational practices that shape this domain (Chesbrough, 2003; Michael 2009).

Third, it is important to recognise that technology cannot 'provide' the right information at the right time, in the right place. People need to assess its accuracy, relevance, quality, they share or withhold it, they can make sense of it, or not, they may discount it, or draw others' attention to information in ways that communicates their judgement about its relevance, quality or import. Technology can greatly enhance these practices, but it cannot replace them, and it can also undermine, obstruct, or transform them.

The ways in which IT are designed, governed and appropriated are thus deeply entangled with how societies conceive of risks, respond to crises, and facilitate freedom. As a result, ELSI rightly stand at the centre of EU-funded research as a core concern, a concern that has been strengthened further through research guidance provided by the European Commission (see, for example, ALLEA 2017). For instance, the FET advisory group to the European Commission has stated that it is:

of utmost importance to incorporate a social sciences and humanities research component in the development of these new technologies from the earliest stage (FET Advisory Group 2016: 2).

This, they argue, includes proactive critiques of potential ethical, legal, and social implications, exploring possibilities for disrupting socio-technical practices, mapping emergent trends in technological values and norms, and most importantly, developing greater reflection on technological innovation and design (FET Advisory Group 2016). Doing so not only improves usability but also the power of innovation.

However, as the work in SecInCoRe shows, it does so only if there is a commitment to incorporate attention to ELSI reflexively and iteratively, not as a 'checklist' that can be ticked off and closed. This need for reflection is not just about informationalisation, but also about communication and engagement across cultural differences.

Many of today's risks do not respect political, geographical or organisational boundaries, leading to an increased diversity of responders called to work together, making cultural reflexivity an important concern:

Intercultural sensibility and aptitudes have to be explored since they refer to the willingness and capacity of people to step outside of their own logic and systems of thought in order to engage with others, and appreciate different cultural narratives

¹ <http://www.tetratoday.com/news/tetras-love-affair-with-the-asia-pacific>



especially if they are not equally valorized or recognized in a given societal context (UNESCO 2014: forward, no page number).

This is linked to calls for more community engagement and public partnerships. The United Nations' Sendai Framework for Disaster Risk Reduction 2015 – 2030 (2015), calls for a 'broader and a more people-centred preventive approach to disaster risk', in which 'disaster risk reduction practices need to be multi-hazard and multisectoral, inclusive and accessible in order to be efficient and effective' (p.10). This should include:

monitoring, assessing and understanding disaster risk and sharing such information and on how it is created; strengthening disaster risk governance and coordination across relevant institutions and sectors and the full and meaningful participation of relevant stakeholders at appropriate levels (p.11)

As new ICTs such as those developed by the SecInCoRe project make such participation possible, they need to support actors to be willing to understand someone else's decision-making process and interests. As importantly, they also need to support actors to develop a critical awareness of their own ways of making sense of the world, so they can better understand how their understandings differ from others in ways that structure everything from accountability to risk classification schemes. While it is not possible to accommodate every possible viewpoint or framework in a single system, it is possible to foster a greater awareness of these differences and provide tools to support engaging difference in ways that finds new values, new partners, and new risks.

To best govern and manage socio-technical innovation in CIS for DRM collaborations, ethical, legal, and social guidance is needed. SecInCoRe – in collaboration with a range of other projects and stakeholders (see <http://isitethical.eu/about-elsi>) – has developed an approach to ELSI reflexive innovation that combines critical investigation with proactive guidance, creative design, and mechanisms for engagement. ELSI in this analysis cannot be uniformly defined for all situations, and it is not possible to provide strict protocols, codes of conduct, rules, or step-by-step instructions. Instead, the aim is to promote responsible scientific and technological innovation, including foresight into ELSI, specifically focusing on beneficence, and justice (Zilgalvis, 2009; see also <http://ec.europa.eu/programmes/horizon2020/en/h2020-section/ethics>). The ELSI Guidance discussed in this document is intended to support translation of awareness of ELSI into good responses in practice and enable ethically circumspect, lawful, socially viable and responsible conduct.

Chapter 3 introduces the 'ELSI Guidance Concept' for hosting, managing, and governing a CIS for collaborative information sharing in DRM. Chapter 4 provides examples of the ELSI Key Terms, describing the methodology used to identify these topics from ethical, legal, and social principles, virtues, and values in the context of collaborative disaster ICT. Chapter 5 similarly describes the ELSI Guidance developed to promote reflexivity in relation to the principles, virtues, and values captured by these Key Terms to support best practices. The sixth (6) chapter explains the forms of interactive and community engagement that have been developed around the Guidance, including a community-based platform, experimental forms of Ethical Impact Assessments, and an offline board game. Chapter 7 provides concrete examples of how the Guidance influenced the design practice within SecInCoRe. Chapter 8 eighth explores how the guidance play a role in larger socio-technical transformations in risk governance. Chapter 9 concludes the deliverable with a description of future work in relation to the ELSI Guidance.



3 ELSI Guidance Concept

Some ethical guidance relating to DRM and ICT already exist, including a variety of codes of conduct and ethics, focusing on humanitarian issues, disaster response and resilience, matters of work practice, and – more recently – on ICT. Many originate from international organizations such as the UN, the International Federation of the Red Cross and Red Crescent (IFRC) (see Büscher et al 2013 for a review). EU organisations have developed codes of conduct for research and innovation (see for example Dratwa, 2014; European Commission, 2013; Pauwels, 2007; Rogerson, 2009; von Schomberg, 2007).

While some of the guidance for DRM addresses key issues relating to ICT such as data protection privacy, informed consent, they also leave many aspects of ethics in information technology design and use unaddressed. They often focus on technology as if it were separate from contexts of design, management, and use, rather than acknowledge the interconnected social, economic, political, cultural, organizational complexities enfolded into it in each stage. They leave unaddressed how the same technology may be used differently in different disasters, in different places, at different times, with different actors, where different, sometimes contradictory, ELSI will emerge. In order to address this misconception, it became necessary to develop new ELSI Guidance that could capture more of the dynamics involved and, with that, develop a new concept and structure for ethical guidance.

The ELSI Guidance described in this deliverable address ELSI that can arise when managing and governing CIS for information sharing in DRM. They combine explanations of Key Terms complemented by Guidance entries to seed an evolving community resource. The ELSI Key Terms are derived from the SecInCoRe inventory and ethical impact assessment (EIA) process. They define, more broadly, the ELSI related to collaborative disaster IT and provide a starting set of general aspects that need to be considered. However, while these aspects help define end-goals, they do not offer clear paths of action. The Guidance entries explore a range of questions to consider to help figure out what about the principles, values, virtues and challenges captured by the Key Terms is important to consider in specific DRM collaborative ICT situations. As a whole, the ELSI Guidance provide resources for those engaged in collaborative, digitally augmented DRM to consider how they might pro-actively notice and address ELSI challenges, or take advantage of ELSI opportunities. The explanations and guiding entries are grounded in empirical research -- ethnographic, interviews, and desk studies – and designed to support better understanding and capabilities to articulate the social, technical, and data practices that enact ELSI, including, among many others, collaboration, security, accountability, privacy, interoperability, and diversity.

Overall, the ELSI Guidance support translation of awareness of issues into best-practice context-sensitive responses. By providing a mix of rules and reflexive questions, they help focus and direct stakeholders who might host, implement, or govern CIS by posing questions that can help them make the best possible decisions regarding ELSI. They do not provide all-purpose solutions, checklists or instructions. Instead they support reflexivity and acknowledge that ELSI emerge dynamically and cannot be addressed in universal ways. The ELSI Guidance are intended to seed an evolving community resource.

3.1 Aims of the ELSI Guidance

The overall aim for the ELSI Guidance is to support real world practices of collaboration and sense-making in ways that critically and creatively address ELSI arising in the increasing informationalisation of DRM, and the need to work across agencies, organisational, political and cultural borders or work with new partners.

By using the ELSI Guidance, those aiming to host, govern, manage, or even design CISs for DRM should gain analytical and reflexive tools with which to consider the challenges and



opportunities enabled by their decisions. These can include how the CIS can support the development of new partnerships; deeper learning from past disasters; more richly and broadly informed risk assessment; challenges to existing practices of establishing meaning, trust, legitimacy, and privacy; and the necessary negotiations between different perspective and forms of political power. By focusing on explanations and reflexive questions, the aim is to provide a resource to help those that are establishing, managing, and governing collaborative ICT for DRM, such as CIS, to proactively identify, understand, and address ELSI.

CIS are understood as interactive environments produced by people for reasoning with information. They need to afford secure information disclosure, withholding, negotiation, sharing, deleting, configuring awareness and collaboration (Bannon and Bødker 1997, Baker and Bowker 2007). The focus in this document is on the collaborative and technical aspects of information sharing in the area of DRM. CISs contain collaborative tools for communication and sharing (Pottebaum, et al. 2016). While all collaboration entails ELSI, CISs enable collaboration at a distance, which also raises new ELSI, such as concerns with how to be aware of others' attention and actions (and 'configure' such awareness, Heath and Luff, 1992). As a result, these situations require different guidance than what may be required for ICT use within a single organization or agency.

In short, the ELSI Guidance DOES:

- support ELSI reflexivity for collaboration supported by ICT
- promote awareness of gaps in existing ELSI guidance, with proposals on how to address these;
- speak to practices of hosting, implementing, and governing CISs for DRM;
- help approach IT in ways that is more circumspect and considers ELSI pro-actively.

The ELSI Guidance DOES NOT:

- speak to collaboration and interoperability in general for DRM;
- address ICT use in general for DRM;
- seek to replace or stand separately from already existing guidelines and codes
- provide universal instructions.

The challenge that ELSI arise in specific contexts (Nissenbaum 1999) means that there are no one-size-fits-all solutions. The Guidance cannot provide simple or definitive rules or step-by-step instructions. However, they can guide stakeholders to carefully consider ELSI and implications of decisions about design, governance and use. The Guidance, thus, are intended to dovetail with existing guidance, supporting their gaps in relation to collaborative disaster IT, while pushing ELSI considerations past rules that will inevitably not fit a situation to ways of approaching problems that are as flexible as DRM practice. In doing so, they aim to support constructive strategies for noticing and dealing with ELSI as they arise. To this aim, the guidance at hand is structured around the development of ELSI reflexivity (Wright 2011; Liegl et al 2016): posing questions, highlighting research, and providing examples that can support deeper understanding of how decisions around CIS adoption, management, and use shape decisions and actions as well as having larger societal implications.

The Guidance treats ELSI as “**matters of concern**” (Latour, 2005) that can shape the outcomes of both IT development for DRM and DRM itself. They build upon a variety of standardisation efforts and existing guidelines (see Tables 2 and 3) that cover aspects related to networked collaboration and information exchange for DRM to add guidance on design, implementation, hosting, and governance processes (both social and technological).



3.2 Background

A starting point for the development of the ELSI Guidance, particularly the list of ELSI Key Terms, have been observations of how ELSI are encountered ‘at the coalface’ of DRM in practice through the Case Studies in the SecInCoRe Inventory of Past Disasters. A second source is core European values enshrined in the European Convention on Human Rights. To develop guidance from these observational and more abstract starting points, we have also drawn upon qualitative empirical and creative design research (with interviews, collaborative design, EIA) in long-term collaborations between practitioners in DRM, technology developers, policy-makers, and social science researchers, as well as several other European research projects.

The European Convention on Human Rights (ECHR) operates as a legally binding human rights instrument alongside the EU-developed Charter of Fundamental Rights of the EU. The ECHR came into force in 1953. It was drafted by the Council of Europe and contains a broad set of principles that are, in turn, interpreted by the courts. The Court of Justice of the European Union (CJEU) references the ECHR with the wider aim of achieving a uniform approach to human rights protections. These principles are the starting point for much existing ethical guidance, including the ones within this document. This is in part because the ECHR protections are relied upon alongside the general legal principles of the EU itself. This is also because cases can be brought before the court established by the Convention, the European Court of Human Rights, or national courts. The judgements are binding and thus integral to conceptions of liability.

However, how they are interpreted into local and organisational practices varies. There are diverse existing standards and guidelines intended to provide DRM practitioners and ICT designers with common benchmarks for various factors that are critical for ‘good’ DRM. In Table 2 below, we have drawn together a selection and we see, for example, that there are a number of organizations that propose principles for practices of multi-agency interoperability, collaboration and coordination. The UK Civil Contingency Act, for example, puts forward principles for practicing effective response and recovery (HM Government, 2013, abridged). We also see that there are a range of ICT ethical codes that are relevant. Such guidelines embody both practical knowledge and ethical principles.

While the ELSI Guidance at hand draws on these standards and principles, it is critical to reiterate that it is not another set of standards or principles and not intended as a complete authoritative set of terms and ‘instructions’. Instead, it is designed as an evolving resource for reflexive critical engagement with ethical, legal and social opportunities, risks, challenges in a fast changing socio-technical landscape. It relies on critical engagement and contributions from those using it (for more about how this works, see chapter 3.3).

Table 2 Existing DRM Standardisation and Guideline Efforts

ISO/TC 223	develops international standards to increase societal security
ISO/TC 292	works with standardization to enhance the safety and resilience of society
WS Agreement TER-CDM	evolving CEN Workshop Agreement on Terminologies in Crisis and Disaster Management initiated by the SecInCoRe-EPISECC-SECTOR-REDIRNET Taxonomy Task Force, First meeting March 2017
Privacy by Design Guidelines	framework to protecting privacy by embedding it into the design specifications of technologies, business



	practices, and physical infrastructures
The UK JESIP - Joint Doctrine: the interoperability framework	sets out a standard approach to multi-agency working
The SATORI CEN Workshop Agreement	ethics Assessment of research and innovation https://www.cen.eu/work/areas/InnoMgmt/Pages/WS-SATORI.aspx
Project Athena: empowering citizens, protecting communities,	to enable and encourage users of new media to contribute to public and individual security in crisis situations, specifically D2.7 "Guidelines for best practice for User Centred Approach"
Guidelines on Cooperation between the United Nations and the Business Sector	a principle-based approach developed in 2000 as a common framework for UN-business collaboration that apply to the UN Secretariat as well as separately administered organs and programmes
Guidelines for cooperation between governments and the private sector for disaster risk reduction	approaches, achievements and challenges, developed under the Work Programme of the Permanent Secretariat of the Latin American and Caribbean Economic System
Disaster Response: Guidelines for Establishing Effective Collaboration between Mobile Network Operators and Government Agencies	guidelines for leverage the expertise of the private sector effectively in order to integrate ICT tools into their response strategies.
IFRC 2011 Introduction to the Guidelines	guidelines for domestic facilitation and regulation of international disaster relief and initial recovery assistance
Global Disaster Alert and Coordination System Guidelines	a cooperation framework between the United Nations and the European Commission in 2004 to address significant gaps in information collection and analysis in the early phase of major sudden-onset disasters
The European Code of Police Ethics (2001)	code of ethics applying to traditional public police forces or police services, or to other publicly authorised and/or controlled bodies with the primary objectives of maintaining law and order in civil society
IFRC (2013) Professional standards for Protection Work	Standards for conduct in responses carried out by humanitarian and human rights actors in armed conflict and other situations of violence, particularly chapter 6 'Managing sensitive protection information' of Professional standards for Protection Work

The ELSI Guidance at hand also draws on existing ethical standards for ICT designers, data analysts, and engineers, a selection of which are presented below.



Table 3 ICT Ethical Standardisation and Guideline Efforts

The Chartered Institute for IT: Code of Conduct	BCS, The Chartered Institute for IT, is a network of IT developers committed to making IT good for society. Its code of conduct sets out basic professional standards http://www.bcs.org/category/6030
The Association for Computing Machinery (ACM)	<i>The ACM Code of Ethics: Guiding Members with a Framework of Ethical Conduct</i> identifies the elements of ACM member's commitment to ethical professional conduct. http://www.acm.org/about-acm/code-of-ethics ,
The European Data Protection Supervisor (EDPS)	EDPS provides a wide range of guidance, predominantly relating to data protection, but it also has the ambition to develop wider ethical guidance, see Opinion 4/2015 Towards a New Digital Ethics https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf
Canada's Association of IT professionals	CIPS has helped strengthen the Canadian IT industry by establishing standards and sharing best practices for the benefit of individual IT professionals and the sector as a whole. Its Code of Ethics and Professional Conduct establishes ethical and enforceable standards, http://www.cips.ca/?q=system/files/CIPS_COE_final_2007.pdf
	American Medical Informatics Association Code of Professional and Ethical Conduct https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3555329/
Association of Information Technology Professionals (AMIA)	The <i>AMIA Code of Professional and Ethical Conduct</i> is meant to be practical and easily understood, ... not intended to be prescriptive or legislative; it is aspirational, and as such, provides the broad strokes of a set of important ethical principles especially pertinent to the field of biomedical and health informatics. http://www.aitp.org/?page=EthicsConduct

These existing standardisation efforts and guidelines cover a range of separate aspects related to ELSI in networked collaboration, information exchange for DRM, and risk governance. They complement our qualitative empirical and creative design research and orientation to the ECHR. What is missing is guidance on how to design, govern, and use collaborative ICT in ways that support real world practices of collaboration and reasoning in DRM in ways that are sensitive and proactive about ELSI.

3.3 Live, Lived, Living ELSI Guidance

Implementation and governance of CIS is best understood as a continuation of socio-technical 'design in use' (Ehn 2008). The ELSI Guidance has been developed as a community platform concept through a collaboration between a range of EU projects (EPISECC, SECTOR, REDIRNET, ConCORDe, EMERGENT, BRIDGE), the Centre for Mobilities Research at Lancaster University and the Public Safety Communications Europe Network (PSCE). It originates from a long-term collaboration between disaster management practitioners, technology developers, policy-makers, social scientists, and legal experts. The result is not a final product to hand over, but - we hope - the beginning of an ongoing process. This Guidance sets the groundwork for a living platform and provides the initial critical mass of content along with an advisory board for the platform's growth. It is intended

to be developed through the contributions and work of those involved in managing and governing collaborative ICT in and CIS for information sharing in DRM.

The platform has been designed to enable dialog and contributions from all interested parties, through comments, examples, and key terms and guidance entries. It is conceived as a 'live, lived, living' platform (Figure 1)

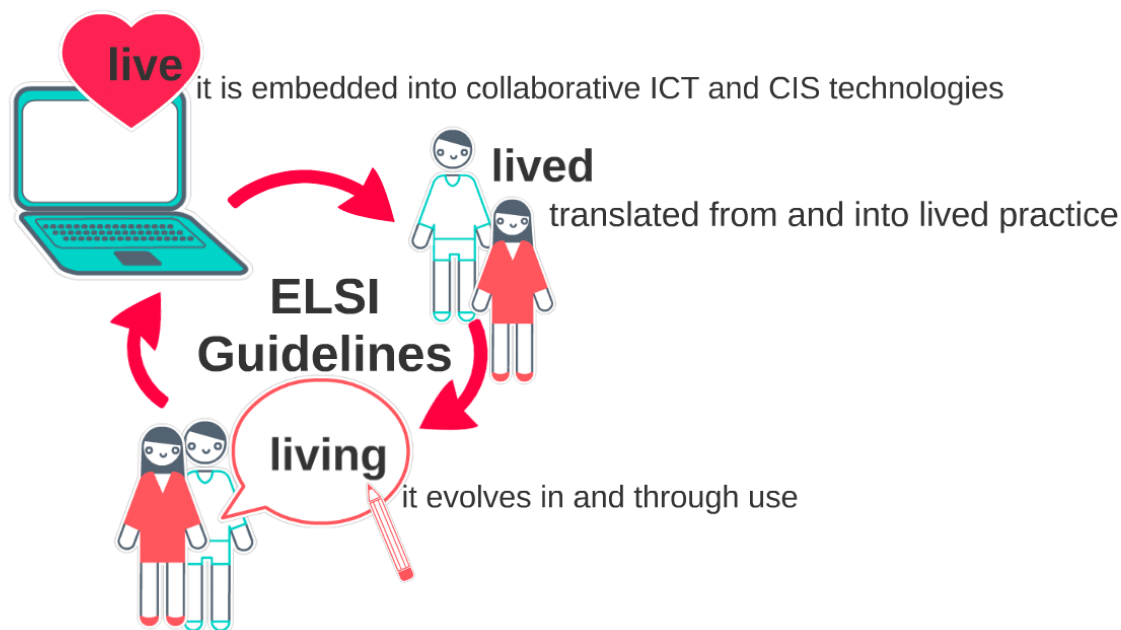


Figure 1 Live, lived, living ELSI Guidance

The Guidance seeks to be '**live**' in the sense that key terms and guidance content are incorporated into (the design of) collaborative ICT and CIS technologies as well as organisational processes. For example, the CEN Workshop Agreement on Terminologies in Crisis and Disaster Management includes key terms, and the SecInCoRe CIS concept embeds ELSI Guidance in a variety of ways (see Chapter 7 for detail). The Guidance is meant to be '**lived**' in two ways. On the one hand, it is derived from a deep understanding of lived practice – an appreciation of how ELSI arise in real world contexts. On the other, it is sensitive to the fact that any guidance must be translate-able into real world practice, where social interactions and moral principles are culturally specific, contested, and can shift in times of disaster. In order for guidelines to be useful they have to be clear in regards to their cultural positioning, and flexible enough to be adapted to specific contexts. Finally, the Guidance is meant to be '**living**', that is open to debate and change, inviting expression and contestation of knowledge and experience from different stakeholders.

3.4 Added Value: Stakeholder Participation and Comments

The ELSI Guidance has been developed in collaboration with a wide range of stakeholders, including, but not limited to:

Barnard-Wills, David - SATORI, Trilateral, UK
Baur-Ahrens, Andreas – Tuebingen University – SECTOR
Behnke, Daniel, TUDO, Germany, SecInCoRe
Blaha, Manfred, Ministry of Interior, Austria
Bonnamour, Marie-Christine - PSCE



Calvert-Lee, Caroline - Civil Contingencies Unit, Portsmouth City Council, UK
ResilienceDirect
Créton-Cazanave, Laurence - UMR Pacte Institut d'études politiques, Grenoble
Delprato, Uberto , IES Solutions, Italy
Emanuilov, Ivo, KU Leuven, Belgium
Force, Pierre , AIRBUS DS SLC, France
Guerin, Flavie, Impulse.brussels, Belgium
Harou, Delphine - European Data Protection Supervisor's Office (EDPS)
Heyman, Rob - imec-SMIT, Vrije Universiteit Brussel
Hirst, Paul, B-APCO, U.K., SecInCoRe
Hildebrandt, Mireille - Professor, Science Faculty, Radboud University Nijmegen and Faculty
Law & Criminology, Vrije Universiteit Brussel
Houbion, Catherine, INFRABEL, Belgium
Huysmans, Kristof - Centre for IT & IP Law, KU Leuven – EPISECC
Ivanc, Blaž, Jožef Stefan Institute, Slovenia
Linke, Harold, HITEC, Luxembourg
Lund, David - PSCE & Broadmap
Marzoli, Marcello, Corpo Nazionale dei Vigili del Fuoco, Italy
Matskanis, Nikolaos , CETIC, Belgium
Miskuf, Robert, PSCE, Belgium
Morentz, James W. Ph.D., Executive Director XchangeCore Open Source Community
Muraszkiwicz, Julia , Trilateral Research , UK
Neubauer, Georg , AIT, Austria
November, CNRS - Valérie Laboratoire Techniques Territoires Sociétés, Paris
Nowak, Andrea, AIT, Austria
Oczko-Dolny, Aleksandra, European Commission, Belgium
Paterour, Olivier, Airbus, France, SecInCoRe
Penman, Dr James I. - CISSP Open Geospatial Consortium
Piquemal, Jean, Individual consultant, Belgium
Pocs, Matthias - ANEC, Germany
Schaefer, Christina, University of Paderborn, Germany, SecInCoRe
Schroers, Jessica, KU Leuven , Belgium
Sofia Tsekeridou, Intrasoft – IMPRESS
Staykova, Toni - FRACP – COncORDE
Testelmans, Rob , Stad Geel, Belgium
Tomas, Robert - Joint Research Centre – INSPIRE
Tudor, Andreea, TEAMNET, Romania
Vasiliu, Irina - DG JUST, EU Commission
Vollmer, Maïke , Fraunhofer INT, Germany
Vreugdenhil , Hanneke, HKV Consultants, The Netherlands
Zimmer , Philippe, INFRABEL, Belgium

Below, we provide a selection of excerpts of statements on the perceived benefits and potential of the ELSI Guidance.

"I like very much the list (of ELSI) and the explanations. Because usually you try to find all these theorems/theories (?) and you can't find them. This is very good." (Tsekeridou)

"We started using the [Inspire] portal from the angle of visualising, [visualising] which members are going to the portal and which data they are using ... So, now, learning [about the ELSI Guidance] throughout the day, we might maybe start thinking about putting, you know, some regulations [like these ones]..." [Robert Tomas, INSPIRE]



*“Personally when I am designing my CIS what I would do, I would read the entire Guidance and cross check what I have in my head and check if I am missing something. I would **validate** my ideas using this. And if I see something that you are missing, because we also having ethical issues, I would provide you with an example. So it works both ways to validate.” [Toni Staykova, ConCORDE]*

“I think it is more about the questions which we direct to this rather than the guideline itself. So, Privacy is not important I think as a guideline in itself but the questions behind it [are]. So, to what extent should you cover privacy in the system? That’s more important than the guideline itself. So you can base your design on the guidance. I think that’s the important part.” [\$]

[responding to a question on whether the Guidance is necessary] *“Absolutely. It brings consistency to the approach from the part of the owners and all the stakeholders. So it would weight your authority to make these demands. Absolutely.” [Finian Joyce]*

“I think it [the ELSI Guidance platform] has a lot of potential because it can take different parameters so it always depends on what is the incident [so it can be tailored to the incident] because in different incidents you have different factors.” [Emma Kollatou, PSCE]



4 ELSI Key Terms

The ELSI Key Terms are a work in progress that is a distillation of ELSI arising in past disasters captured in the SecInCoRe Inventory, principles expressed during SecInCoRe co-design Workshops, EIAs, and PIAs, unearthed, and emerging within the actual practices of emergency response, and extensive literature reviews. This was started by mapping out and reviewing the landscape of existing ethical frameworks, see Table 2 and Table 3. The most widely used set of humanitarian principles is provided by the IFRC and many of the principles expressed there for a self-policing code of conduct with humanitarian intention are echoed by codes that focus more narrowly on disaster and emergency response. For example, *The European and Mediterranean Major Hazards Agreement* proposes an ethical code of conduct for all agencies involved in emergency response (Prieur 2009). While it is informed by the numerous ethical frameworks, as outlined above, it does not simply replicate them.

What follows is a first attempt at defining a catalogue of ethical key terms for multi-agency emergency management that provides insight into the values aspired to in current practice. It is not a complete list of ethical, legal, and social issues that might be relevant to DRM or to IT design and use. The key terms collected in this list engender the challenges and opportunities in implementing, hosting, managing, and governing collaborative IT for DRM. This list is also an inventive method – alphabetical in its ordering but experimental, emerging and perpetual in its nature – which intends to provoke further conversations, further debates and further ELSI to be added (Lury and Wakeford 2012; Phillips 2012).

4.1 Key Terms Overview

The Key Terms provide an overview of key ELSI involved in CIS-facilitated collaboration for DRM. Each provides a short definition that we have drawn together from different sources, with reference to those sources, a bulleted list of key aspects to consider, and a list of guidance entries that are particularly relevant to help, more practically, address those aspects.

The complete list of key terms currently includes: Accessibility, Accountability, Adaptability, Anonymity, Autonomy, Beneficence, Cooperation, Data Protection, Disclosure, Diversity, Equality, Fairness, Freedom of Association, Freedom of Expression, Freedom of Movement, Humanity, Impartiality, Inclusiveness, Informational Self-Determination, Justice, Leadership, Non-Discrimination, Privacy, Proportionality, Respect, Responsibility, Security, Solidarity, Stewardship, Transparency, and Trust. They can be examined at www.islTethical.eu. Below, we present examples, to illustrate the format.

In some respects the key terms are an entry point into the more expansive SecInCoRe Inventory, which includes ELSI arising in DRM more widely. The Key Terms can support users who are still thinking about how to address specific principles but might not yet have articulated the challenges or opportunities they will face as they engage with collaborative ICT.

4.2 Examples

This section outlines five Key Terms that illustrate the composition of the Key Terms entries. A full set of the current list and status is available at www.islTethical.eu.



4.2.1 Accountability

Accountability refers to being answerable for one's choices and actions and recognising one's role and being responsive to the, sometimes divergent, expectations attached to it. It also applies to technology in the sense that infrastructures and algorithms should 'account for' their affordances and actions in ways that are intelligible to people. Recognising the role of individuals and organisations involved in CIS design, management, and use necessitates appreciating the responsibility shouldered by each individual and group involved. This includes considering how actions could impact those engaged in the CIS as well as the greater society.

- Be cognisant of and take responsibility for actions in information sharing.
- Be responsive in accordance with the duties of your role.
- Consider the potential impacts of behaviour, research, and sharing outcomes.
- Be aware of your expectations of others' capacities, focus, and responsibilities and how they affect your own decisions.

Sources

Buttarelli, G. (2016) The accountability principle in the new GDPR, Speech at the European Court of Justice, Luxembourg, 30 September.
https://edps.europa.eu/sites/edp/files/publication/16-09-30_accountability_speech_en.pdf

European Data Protection Supervisor (2016) *Guidelines on processing personal information in administrative inquiries and disciplinary proceedings*.
https://edps.europa.eu/sites/edp/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf

Petersen, K. et al. (2015) *D2.02 ELSI guidelines for collaborative design and database of representative emergency and disaster*. SecInCoRe EU Deliverable. <http://www.secincore.eu/publications/deliverables/>

Satori (2016) *Ethics assessment for research and innovation - Annex A*. CWA SATORI-1:2016

Tenenberg, J., Roth, M.-W., Socha, D. (2016) "From I-Awareness to We-Awareness in CSCW". *Computer Supported Cooperative Work (CSCW)*. V. 25(4-5): 235-278.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). [Information accountability](#). *Communications of the ACM*, 51(6), 82–87. <http://doi.org/10.1145/1349026.1349043>

Related Guidance

Justifying Exclusion
Accountable Anonymity
Transparency of Data Processing
Data Controllers
Technology and Power

4.2.2 Diversity

The EU has a long tradition of deliberative collaboration that builds on long-term



mutual respect and understanding between partners, and broader values of ‘unity in diversity’. EU objectives should always leave sufficient implementation room so as to allow for national diversity and flexibility. To do this, there needs to be support for translation between roles, languages, IT systems, etc. to make a CIS useful. There also needs to be considerations in how the data sharing structures are established and how diverse needs and perspectives shape how data is sought. Differences need to be made visible and available to enable one party to understand what is implied by another party’s incident report or information request. Diversity is linked to ‘subsidiarity’, that is, the principle of devolving decision-making to the lowest possible level whilst supporting coordinative action at a higher level ([EU Glossary](#)).

- Support translation between roles, languages, situations, and IT systems.
- Consider how data sharing structures address diverse needs and perspectives
- Make differences in practices and meanings visible
- Attend to the principle of subsidiarity

Sources

Baker, K. S., & Bowker, G. C. (2007). Information ecology: open system environment for data, memories, and knowing. *Journal of Intelligent Information Systems*, 29(1), 127–144. Retrieved from <http://connection.ebscohost.com/c/articles/26147317/information-ecology-open-system-environment-data-memories-knowing>

Bowker, G., & Star, S. L. (2000). *Sorting Things Out: Classification and Its Consequences*. Cambridge, Massachusetts: MIT Press.

Edwards, P. (2010). *A Vast Machine*. Cambridge, MA: MIT Press.

Jordan, K., & Lynch, M. (1992). The Sociology of a Genetic Engineering Technique: Ritual and Rationality in the Performance of the “Plasmid Prep.” In J. Fujimura & A. Clarke (Eds.), *The Right Tools for the Job* (pp. 77–114). Princeton: Princeton University Press.

Ramirez, L., Buscher, M., & Wood, L. (2012). *Domain Analysis - Interoperability and Integration*. Bridge project Deliverable D2.2.

Rolland, K., Hepso, V., & Monteiro, E. (2006). Conceptualizing Common Information Spaces Across Heterogeneous Contexts: Mutable Mobiles and Sideeffects of Integration. *CSCW '06 Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, 493–500.

Schmidt, K., & Bannon, L. J. (1992). Taking CSCW seriously. *Computer Supported Cooperative Work*, 1(1), 7–40. <http://doi.org/10.1007/BF00752449>

Related Guidance

Recognising Relevant Collaborators
Public Engagement
Multiple Perspectives
Different Understandings of Risk
Cultural/Linguistic Differences
Goal Diversity



4.2.3 Equality

According to the [European Convention for the Protection of Human Rights and Fundamental Freedoms](#), all persons are equal before the law and entitled to equal protection. Disaster Risk Management entails a need for more dedicated action to tackle underlying disaster risk drivers, such as the consequences of poverty and inequality.

- Promote the equality of all persons through collective attention to a general prohibition of discrimination.
- Ensure that different groups of people to have a similar social position and receive the same treatment.
- Ensure equality of contribution and access to common information spaces, including elimination of the hierarchical power structures that dominate most other areas of our lives.

Sources

Council of Europe (1950) European Convention on Human Rights.
http://www.echr.coe.int/Documents/Convention_ENG.pdf

UNISDR. (2015). *Sendai Framework for Disaster Risk Reduction - UNISDR*.
Retrieved from <http://www.unisdr.org/we/coordinate/sendai-framework>

Related Guidance

Access and Fairness
Digital Divides
Technology and Power
Authority, Control and Participation
Facilitating Dialogue



4.2.4 Privacy

Privacy and data protection are often used as interchangeable terms and, indeed, there is no absolute consensus in relation to these concepts. At a basic level, privacy can refer to the appropriate use of data relating to an individual in each specific context and, at times, in relation to an expectation of privacy. The term “data protection” is used extensively throughout EU legislation and relates to the management of data in, for example, a CIS. The EU’s updated data protection framework has included more privacy-enhancing measures such as the right to delete, that provide end users with enhanced control over the use of their data. All of these concepts and complex privacy practices need to be embedded into CIS design.

- Render identifiable information about research participants confidential
- Protect collected data from unauthorised access and store participant data securely
- Be aware of the difference implications between the law, algorithms that manage the law, and persons that interpret the law.
- State clearly the intentions for what privacy provides and to what effect.
- Include systems that enable end users with identifiable personal information in the CIS to assert their rights over this information.

Sources

Büscher, M., Perng, S.-Y., & Liegl, M. (2015). Privacy, Security, Liberty: ICT in Crises. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*.

Dratwa, J. (Ed.). (2014). *Ethics of Security and Surveillance Technologies* (Opinion no, pp. 1–165). Brussels: European Group on Ethics in Science and New Technologies to the European Commission.

Satori (2016) Ethics assessment for research and innovation - Annex B. CWA SATORI-1:2016

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, 51(6), 82–87. Retrieved from http://dl.acm.org/ft_gateway.cfm?id=1349043&type=html

Related Guidance

Privacy and Personal Data Protection
Security in CIS
Transparency of Data Processing
Ethical and Privacy Impact Assessment
Protecting the Rights of Data Subjects
Data Protection Impact Assessments



4.2.5 Trust

Trust is an ongoing practice that requires more than simply sharing resources; to trust is to voluntarily open oneself up to risk and vulnerability. It is supported by intellectual honesty, knowing one's limits, and having the humility and integrity to consult others. Trust is practiced through respect for the reports of others and willingness to base action on them. Trust in technology emerges when expectations are regularly met and grows as technologies become more dependable. Trust in CISs may be encouraged through doing what is says it does (and not less or more) and demonstrating repeatability, predictability, dependability, and, thus, reliability.

- Respect the reports of others and be willing to base actions upon them
- Consult others when there are uncertainties
- Identify positive expectations and enable them to be regularly met

Sources

Büscher, M., Mogensen, P.H. and Kristensen, M., 2009. When and how (not) to trust IT? Supporting virtual emergency teamwork. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, 1(2), pp.1-15.

https://www.researchgate.net/profile/Monika_Buescher/publication/220295328_When_and_How_Not_to_Trust_It_Supporting_Virtual_Emergency_Teamwork/links/0912f507e2adf23c7f000000.pdf [Accessed 06/04/2017]

Clarke, K., Hardstone, G., Rouncefield, M., Sommerville, I. (2006). *Trust in Technology: A Socio-Technical Perspective* (Computer Supported Cooperative Work). New York: Springer-Verlag.

Friedman, B., Khan Jr, P.H. and Howe, D.C., 2000. Trust online. *Communications of the ACM*, 43(12), pp.34-40.

Petersen, K. et al. (2015) D2.02 ELSI guidelines for collaborative design and database of representative emergency and disaster. SecInCoRe EU Deliverable. <http://www.secincore.eu/publications/deliverables/>

Shneiderman, B., 2000. Designing trust into online experiences. *Communications of the ACM*, 43(12), pp.57-59. <http://www-lb.cs.umd.edu/~ben/papers/Shneiderman2000Designing.pdf> [Accessed 06/04/2017]

Related Guidance

Facilitating Dialogue
Justifying Exclusion
Transparency of Data Processing
Accountable Anonymity
New Partnerships

4.3 Summary

This Chapter has described the 'Key Terms' component of the ELSI Guidance and provided a listing of all key terms as up-to-date on 26 April 2017. The current listing is evolving and



available at www.isITethical.eu. The way in which ELSI arise around these key terms is concretely addressed in specific guidance entries, described in Chapter 5 below.



5 ELSI Guidance

The key terms alone cannot provide instructions on how to address them or even achieve the principles stated within, because ELSI are contextual and often complex. The ELSI Guidance aims to support such action by guiding stakeholders on what to notice and what consider in relation to these key terms. To this aim, the Guidance is structured around the development of ELSI reflexivity: providing questions, insights from practice and research, with examples that help to illustrate how decisions around collaborative IT implementation, management, and governance can shape DRM in practice as well as larger societal contexts. The guidance offers advice on why specific issues are important to address.

Because collaborative disaster IT require the negotiation of diverse perspectives, they can complicate the relationships and politics between organisations, aggravate sensitive cultural problems, interfere with the ability to support humanitarian values, and blur physical boundaries in ways that make violations less clear cut. The Guidance supports those facing and aiming to address these challenges. They offer insight into and support for what kinds of interaction, even if intended as collaboration, might in fact lead to fragmentation, exclusion and distrust. As importantly, they help support seeing the potential in new tools, such as opportunities for more inclusive risk governance, enhanced security, and better ways of exercising solidarity.

This chapter describes the guidance entries component of the ELSI Guidance and provides five examples to illustrate their structure and content.

5.1 ELSI Guidance Structure and Template

The guidance entries component of the Guidance is divided into five chapters, each with subchapters:

Table 4: ELSI Guidance Table of Contents for Guidance Component

Chapter 1: Establishing a CIS Framework	Producing Meta-Data
Codes of Conduct & Ethics	Information Mapping
Goal Diversity	Chapter 4: Organisational Interoperability
Different Understandings of Risk	Recognising Relevant Collaborators
Responsibilities for Data	Cross-Boundary Collaborations
Authority, Control, and Participation	New Partnerships
Chapter 2: Collaborative Governance	Multiple Crisis Management Models
Decision Making	Multiple Perspectives
Responsive Governance	Cultural/Linguistic Differences
Public-Private Collaborations	Avoiding Fragmentation
Distribution of Responsibilities	Contextual Reasoning
Facilitating Dialogue	Configuring Awareness
Access and Fairness	Articulation Work
Justifying Exclusion	Mission creep
Security in CIS	Public Engagement
Transparency of Systems	Chapter 5: Lawful Conduct
Transparency of Data Processing	Privacy and Personal Data Protection
Accountable Anonymity	Exceptions and lawful processing
Technology and Power	Data protection when crossing borders
Ethical and Privacy Impact Assessment	Data Controllers
Chapter 3: Data Interoperability	Protecting the Rights of Data Subjects
Digital Divides	Data Protection Impact Assessments
Data Standards	Liability
Data Quality	



Each is divided into sub-chapters on specific aspects that arise in relation to the theme. In each guidance a brief explanation is followed by a set of reflexive questions, a section with further information, practical examples, and reference to resources. The platform is set up to allow the guidance to grow through contributions from the practitioner and develop community as well as researchers and other stakeholders as express in Chapter 3.3 for which a system of governance has been established in order to monitor and support contributions (see <http://isitethical.eu/contributors-corner> for how this works on the platform). This means, over time, the list of themes and aspects may grow and change, as well as the individual content.

5.2 Examples

In this section we provide five examples of the Guidance, one from each chapter. The full list and current status is available at www.isitethical.eu.



5.2.1 Goal Diversity

Hint: Working with shared and divergent goals

CISs need to afford negotiation between the various stakeholders' goals, interests and concerns. Participants should be supported in taking one user's specific way of knowing risks or incidents and translating it to be understood by fellow users with different backgrounds and experiences. This is because CISs put into conversation information gathered using several different methods and put together information that is intended to achieve different goals by the various actors involved. While standards, procedures, and classification schemes are fundamental to sharing across organisational and institutional boundaries, a CIS needs more to support collaboration. It needs to involve the identification of the key overarching goals of the system itself, as well as of the governing bodies, organisations, and individual users of the system.

Guiding Questions

What goals do you have that others might not share? What goals are interrelated?

How are goals, interests, concerns communicated?

How can the CIS help clarify shared or divergent interests and concerns?

How can the CIS support collaboration amongst actors with competing goals?

How can the CIS encourage the articulation/translation of these goals?

How can these articulations be tied to data as it is gathered for, and used within, the CIS?

Further Information

As the amount of linked data increases, so too does the diversity of data. Stakeholders often find it difficult to make sense of the various data coming their way, since they do not have the same focus in their engagements with the information as those who entered it into the system. To be useful, the CIS needs to provide a flexible, ever changing, yet self-evident standard of classification and meta-data to accommodate for the increase in data without abstracting and erasing the diversity.

Examples

In a study entitled 'Understanding Complex Information Environments' Van House, Butler, and Schiff (1998) explore the working patterns around information sharing and collaboration in relation to California watershed planning and examine how these ideas might play out in a CIS. They describe the watershed planning process and CIS as "distributed physically in time and space, and logically in terms of control; and with no omniscient agents organizing the work" (p. 336). The engagements they observed involved a range of stakeholders, from government agencies, resource-based industries such as agriculture and timber, environmentally-based industries such as recreation, landowners, and non-government environmental groups, and community groups. The planning took place at state, regional and local levels, often with the need to manage competing interests. The goal for these interactions in relation to watershed planning were for these stakeholders to come to as much of a shared understanding of the current state of their watershed regions as possible. From this they hoped to produce a common set of expectations from future actions and agreements for overarching goals. Van House et al. found that the shared information was not just used for decision-making but equally "for defending points of view and persuading and educating others" (1998, p. 337), illustrating the qualities of information as a 'boundary



object'. In doing so, the different stakeholders used different data and privileged different uses of the data.

Concerns:

- Fear of losing the legitimacy of their communities of practice that would limit their authoritative voice.
- Fear of the use of their data in unintended ways because the data were disassociated from their site of production and thus made to mean new things without consideration for the specifics from which they derive.

Solutions:

Using descriptive meta-data that aimed made it possible to calibrate measurements, terminology and data elements across the range of information provided within the CIS.

Using established mapping or reporting structures supported stakeholders in knowing they were appropriately combining different data from different sources. Van House et al. do note that, "whether such detail can be sufficiently specified is, however, debatable" (p. 340).

Tags: Cooperation, Diversity, Fairness, Impartiality, Solidarity

Resources

Cooper, A. and Reimann, R. (2003). *About face 2.0: The essentials of interaction design*. John Wiley & Sons

Joshi, A. Usability Goals Setting Tool. Available at <http://www.idc.iitb.ac.in/~anirudha/ugt.htm>

Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social Studies of Science*, 19(3), 387. Also available at http://www.lchc.ucsd.edu/MCA/Mail/xmcamail.2012_08.dir/pdfMrgHgZULhA.pdf

Tognazzini, B. (2003). First principles of interaction design. Available at <http://www.asktog.com/basics/firstPrinciples.html> <http://www.usability.gov/how-to-and-tools/methods/develop-plan.html>

Usability.gov Project team roles and responsibilities. Available at <http://www.usability.gov/how-to-and-tools/methods/project-team.html>

Van House, N. A. Van, Butler, M. H., & Schiff, L. R. (1998). Cooperative Knowledge Work and Practices of Trust: Sharing Environmental Planning Data Sets. *The ACM Conference On Computer Supported Collaborative Work, Seattle, WA November 14-18*, 335–343. Doi: [10.1145/289444.289508](https://doi.org/10.1145/289444.289508).

Wolbers, J., & Boersma, K. (2013). The Common Operational Picture as Collective Sensemaking. *Journal of Contingencies and Crisis Management*, 21(4), 186–199. <http://doi.org/10.1111/1468-5973.12027>. Also available at https://www.researchgate.net/profile/Kees_Boersma/publication/259544396_The_Common_Operational_Picture_as_Collective_Sensemaking/links/547c513d0cf2a961e48a00de.pdf



5.2.2 Decision Making

Hint: Collaboratively developing decision and accountability processes

Collaborative governance brings public and private stakeholders together in collective forums with public agencies to engage in decision making. It is important that different stakeholders consider their common goals and objectives, including their motivation for collaboration, and define a framework through which they can achieve, monitor, and assess these goals and objectives. This can involve clarifying the formal/informal rules and norms of working together, developing decision making procedures, defining leadership models to help facilitate the collaborative process, and setting a framework for managing ELSI and other lessons learned as they arise. This also includes thinking about the next generation of actors, developing clear mechanisms for transparency and accountability for all organisations involved, and establishing repercussions for breaches of the governance structure.

Guiding Questions

How is leadership determined?

How does the CIS design support social and material practices of decision-making?

How can the CIS support decision-making that considers diverging interests, (unknown) lessons learnt and future needs?

Is the CIS biased towards consensus or other forms of decision making?

What mechanisms or strategies are in place to support contestation?

Further Information

As the uncertainties and frequency of disasters grow, disaster risk management relies on a wider set of public and private partners, encompassing federal, state, and local levels of government, as well as businesses, voluntary organizations and citizens. A range of questions about coordination strategies, systems, practices and attitudes arise at this juncture: 'Are emergency managers trained to work with these new actors? How committed are they to seeking new partners to assist in disaster planning and response? What policy guidance do they need? How prepared are they to work within broader partnerships? How familiar and comfortable are they with the different norms, cultures, and interests involved? Do their agencies have the budget, background, and training to involve these groups on an ongoing basis? How will decisions be made, and by whom? (see McGuire et al 2010)

Collaborative governance is often oriented towards consensus (Ansell and Gash 2007). However, consensus can be difficult in such a setting, and, in fact, it can be undesirable. Decision-making for disaster risk management needs to accommodate the possibility to negotiate different interests and forms of knowledge. Governance processes need to 'create a space in which different interests and knowledges can be negotiated, contestation is possible, power relations are being put into question and no victory can be final' (Mouffe in DiSalvo 2010). This requires accepting that conflicting views may be inherent to the process of good disaster risk management, conflicts that can be exacerbated by cross-border collaboration (see Storni 2013).

In her review of democratic risk governance Jasanoff argues that command and control attempts at 'disciplining the incalculable through sophisticated forms of calculation' enact ill-advised hubris (2010), and she argues for a shift from disaster risk management to democratic risk governance. This does ***not*** mean abandoning command and control. Jasanoff envisages engagement of different actors as complementary to formal efforts and



shows that risk governance requires not only expert professionalism and broad-based engagement with local knowledge, but also an understanding of how vulnerability and resilience reflect and enact political choices that affect individuals and communities unequally. (for further discussion, see Büscher et al 2017, in press).

Examples

Decisions between Public-Private Partnerships: Chen et al (2013) show that in public-private contractual partnerships for critical infrastructure, challenges to decision-making often arise because high degrees of uncertainty and the different types of discretion provided to different organisations. This means that contracts, that explain specific roles within collaborations, are often incomplete and potentially involve frequent renegotiations, posing challenges for maintaining an authoritative decision making structure as well as for the necessary disclosure of information within CISs. These interactions create high risks of opportunism and transaction costs (e.g., monitoring, enforcement and conflict resolution) which could also affect the aims decisions made. Joint ventures with diverse stakeholders require high levels of trust and awareness of each other's goals, where information sharing may sometimes need to be very carefully calibrated and contested and may require long-term relationship building and incentive structures that align the interests of public and private collaborators.

Long term effects: Fortun's study of the mismanagement of risk in the city of Bhopal (2011) illustrates the value of more flexible epistemological and moral technologies: in the aftermath of the disaster at the Union Carbide India Limited company, it was not enough to consider the risk of harmful chemicals on the basis of individual substances affecting individual human bodies at a particular point in time. Interactions between multiple substances and long-term interdependencies had to be taken into account, and the evaluation of risk and damage changed over time. The deliberative learning potentially enabled by CIS allows a focus on the unequal distribution of risk and enables collective reflection and evaluation of explanations and approaches, a different form of decision making than is possible in a top-down authoritative system (Jasanoff 2003). Deliberative learning brings to the table a form of 'social learning where the knowledge of the expert and that of concerned laypeople do not mutually exclude one another', a framework for interaction that resonates with the debates about the need to support contestation (Storni 2013).

Tags: Accountability, Trust, Stewardship, Beneficence

Resources

- Ansell, C. and Gash, A., 2008. Collaborative governance in theory and practice. *Journal of public administration research and theory*, 18(4), pp.543-571. <http://doi.org/10.1093/jopart/mum032> Also available at http://marphli.pbworks.com/w/file/attach/55667103/Collaborative_governance_theory.pdf
- Büscher, M., Kerasidou, X., Petersen, K. and R. Oliphant (2017 in press). 'Networked Urbanism and Disaster', in Freudendal-Petersen, M. and Kesselring, S. (Eds). *Networked Urban Mobilities*. Springer.
- Chen, J., Chen, T. H. Y., Vertinsky, I., Yumagulova, L., & Park, C. (2013). Public-Private Partnerships for the Development of Disaster Resilient Communities. *Journal of Contingencies and Crisis Management*, 21(3), 130–143. <http://doi.org/10.1111/1468-5973.12021>



- Debreceeny, Roger S. (2013) Research on IT Governance, Risk, and Value: Challenges and Opportunities.. *Journal of Information Systems*, 27(1):129-35.
doi: <http://dx.doi.org/10.2308/isys-10339>.
- DiSalvo, C. (2010) Design, democracy and agonistic pluralism, Proceedings of the Research Design Society Conference, Montreal, 6. Available at <http://blog.ub.ac.id/irfan11/files/2013/02/Design-Democracy-and-Agonistic-Pluralism-oleh-Carl-Disalvo.pdf>
- Fortun, K. (2011). Remembering Bhopal, Re-figuring Liability. *Interventions: International Journal of Postcolonial Studies*, 2(2), 187–198.
<http://doi.org/10.1080/136980100427306>
- Hartman, C. and S. G. D. (2006). *There is No Such Thing as a Natural Disaster: Race, Class, and Katrina*. New York: Routledge.
- ISO/IEC 38500:2015, see: <https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en>
- Jasanoff, S. (2003) Technologies of Humility: Citizen Participation in Governing Science. *Minerva* 41, no. 3, 2003: 223–244. Also available at doi:10.1023/A:1025557512320
<https://eclass.hua.gr/modules/document/file.php/GEO200/JASANOFF,%20CITIZEN%20PARTICIPATION%20IN%20GOVERNING%20SCIENCE.pdf>
- Jasanoff, S. (2010) Beyond Calculation: A Democratic Response to Risk. In G. Lakoff (Ed.), *Disaster and the Politics of Intervention*, 14–41. New York: Columbia University Press.
Doi: <http://www.jstor.org/stable/10.7312/lako14696>
- Klinenberg, E. (2002). *Heat Wave: A Social Autopsy of Disaster in Chicago*. University of Chicago Press.
- McGuire, M. Brudney, J. L., & Gazley, B. (2010). The “New Emergency Management”: Applying the Lessons of Collaborative Governance to Twenty-First-Century Emergency Planning. In T. R. O’Leary, D. Van Slyke, & S. Kim (Eds.), *The Future of Public Administration around the World*, 117–128. Washington, DC: Georgetown University Press.
- Acklesh, P., Green, P. and Heales, J. (2013). On Governing Collaborative Information Technology (IT): A Relational Perspective. *Journal of Information Systems*, 27(1):237-59. **doi:** <http://dx.doi.org/10.2308/isys-50326>
- Storni, C. (2013, June 9). Design for future uses: Pluralism, fetishism and ignorance. Proceedings of the Nordic Design Research Conference 2013: Experiments in design research. Copenhagen, Denmark and Malmö, Sweden, June 9, 2013 – June 12, 2013.
<http://www.nordes.org/opj/index.php/n13/article/view/276>



5.2.3 Data Standards

Hint: Rules for data quality, storage, sources

Data standards are the rules and definitions by which content is described and recorded as data. To share or store data there must be standards in order for the various technological systems along the way to be able to incorporate these data during and after the storing and sharing processes. However, one effect of increasing the range of data sources and people interpreting data is a need to create these rules in ways that can be applicable from one situation to the next. However, just having data in the same format does not mean it has the same meaning for everyone using it. Standards and classification systems are codifications of value systems and social practices and thus these decisions cannot be based, in full, on what is technologically possible but also need to consider the social and ethical implications of the choices made in categorising, classifying, and sorting data for sharing.

Guiding Questions

How far down the response chain does data need to go? How broad in range does the data need to be?

Are all relevant stakeholders being included in the creation or adaptation of the data taxonomy?

Is there a review process of the standards, codification and taxonomy?

How can the data standards allow for a diversity of expressions of accuracy, trust, and quality? How can they facilitate the translation between these expressions?

Further Information

Data standards can provide data integrity, consistency, minimize redundancy, and help clarify ambiguities. They can act as global reporting mechanisms. They make it possible for more than one person to gather and use data. They can also make it possible for technology designers or service providers to better understand the needs of disaster risk management. It is crucial for data protocols, via standards, to be compatible and complementary for cross-border interoperability or the ability to receive direct operational support from other countries.

However, different practices, such as local risk analysis, often are best supported by different standards. It also leads to the need to ensure control of the information chain, from validation of raw data, finding and sharing mechanisms, to processing so as to maintain coherent and reliable information. Moreover, carrying a data standard or classification from one place to another or one situation to another is an act of imposing one set of values onto another, as well as places potential limits on data use. When working at the intersection of multiple ontological frameworks, the challenge becomes one of determining what type of knowledge gets included into standards and systems of classification in ways that keep diversity and ambiguities with the data. Some of this knowledge cannot be reconciled technologically with rules or via shared standards, but needs constant “intermediation” by liaisons. That’s only possible if there is some level of transparency in the standards, in the system that organises the data for data sharing.

Examples

Flood Risk Standards: In UK flood risks assessment, data about flooding is gathered with a +20% rule, a rule intended to create a uniform approach to accounting for water flow and future floods. This rule is a standard for scaling historical records of peak flow across data



from similarly sized catchments in the UK. However, combined with the models, restricted number of experts, and software used, the rule, which does not change the frequency of flooding, affects the probability of flooding occurring and cause flood risks to be constructed in specific ways. UK Environmental Agency consultants recognized that this impacted their practice. As one stated “Models determine what is modelled’ because different models represent different elements of the flood system” (Lane et al: 1801). Models, standards, and individual practices change what questions are able to be asked, and thus the answers. The answers can be so different as a result, different Environmental Agency consultants could provide very different 100 year flood levels for the same catchment.

As another consultant noted:

“their flood maps only show their estimates of flooding of water which comes out of rivers because the rivers are overfull. It doesn’t show the flooding caused by water trying to get into the rivers because it rains too much. And a lot of the flooding certainly in places like Hull and part of what happened in Sheffield this summer [2007], was not water coming out of the rivers. In Hull it wasn’t at all. It was water that fell on the ground and couldn’t get into the rivers. And then those maps don’t show that.” (Lane et al: 1801-1802).

While the standards framed risk in very particular ways, they did not override the nuances of the models used, software available, and individual expert experience. As result, two experts discussing the same standards assumed very different risks.

Compiling risks via data standards: In a study examining chemical pollution after Hurricane Katrina, Frickel (2008) compiles data to show who data standards used to define sampling points for legacy chemicals did not match well with where chemical activity had taken place. The legal regulations in the U.S say the Environmental Protection Agency has to check the non-residential areas (e.g. areas where there are factories, etc) that were flooded: look at where chemicals might have been polluted in the flooding. But Frickel found that mixed use areas did not equal non residential. That meant that areas that had in recent history had industrial activity but were now either partially or fully residential. Those were not included in the data standards for sampling points yet were the source of many health problems for an already marginalised population.

Tags: Security, Inclusiveness, Transparency, Trust, Data Protection

Resources

Baker, K. S., & Bowker, G. C. (2007). Information ecology: open system environment for data, memories, and knowing. *Journal of Intelligent Information Systems*, 29(1), 127–144. Retrieved from <http://connection.ebscohost.com/c/articles/26147317/information-ecology-open-system-environment-data-memories-knowing>

CEN. (2017) Water quality in the loop of European Standardization. https://www.cencenelec.eu/news/brief_news/Pages/TN-2017-006.aspx

European Commission (2014). *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on a new EU approach to the detection and mitigation of CBRN-E risks*. Brussels, 5.5.2014 COM(2014) 247 final. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/explosives/docs/20140505_detection_and_mitigation_of_cbrn-e_risks_at_eu_level_en.pdf



Frickel, S. (2008). On Missing New Orleans: Lost Knowledge and Knowledge Gaps in an Urban Hazardscape. *Environmental History*, 13(4), 643–650.

High Representative Of The Union For Foreign Affairs And Security Policy (2016). *Joint Staff Working Document EU Efforts to strengthen nuclear security*. Brussels, 16.3.2016 SWD(2016) 98 final
<https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/10102-2016-98-EN-F1-1.PDF>

Lane, S., Landström, C., Whatmore, S. (2011) "Imagining flood futures: risk assessment and management in practice". *Phil. Trans. R. Soc. A*, v. 369: 1784–1806.

Open Geospatial Forum Discussion Papers. See:
<http://www.opengeospatial.org/docs/discussion-papers>

USGS (2017) *Data Management: Data Standards*. See:
<https://www2.usgs.gov/datamanagement/plan/datastandards.php>



5.2.4 Recognising Relevant Collaborators

Hint: Supporting the ongoing discovery and inclusion of new partners

The inclusion of a wide range of stakeholders in a CIS is not only an issue of democracy, it also affects the response by bringing in new knowledge and improves trust in the disaster response within the affected community. How such participation is managed in a CIS and by whom, along with questions of inclusion/exclusion are key considerations. Deciding whose participation is relevant in a collaboration can be complex - as it depends on how one defines risk, responsibility and capacity for response - and it might change over time. Consequently, when establishing a collaboration it is necessary to consider the mechanisms by which partners are identified and changed through CIS interaction.

Guiding Questions

When setting up the collaborative platform, how can one ensure that all relevant stakeholders are invited to participate either right from the beginning or at a later stage?

Deciding whose participation is relevant might change over time. Are there any procedures in place for re-evaluating this along the way?

How will access be modulated to account for different information needs?

Further Information

While crisis management has been traditionally the field of first responders, we now know that there is a wide range of stakeholders other than core responders -- such as NGOs, private companies, or digital humanitarians – can, and do, play a vital role in crisis management. However how and in what capacity different stakeholders participate varies depending on the situation and the country, but also how one defines risk and the disaster and so what sort of solutions/responses might be set in motion. In response to this, one of the key principles in the United Nations *Sendai Framework for Disaster Risk Reduction 2015 - 2030* states: 'Disaster risk reduction requires an all-of-society engagement and partnership' (UNISDR 2015). Without considering how publics form in relation to risks, it becomes difficult to protect and serve the public.

A study of 22 European countries as part of the ANVIL FP7 (<http://anvil-project.net/>) project found that the extent to which stakeholders such as public organisations, the private sector, individual citizens are involved in response efforts varied significantly between countries. These differences were based largely on cultural, historical and political traditions, such as whether there is a strong corporatist state tradition, or whether there is a libertarian heritage which favours more flexible arrangements, hence affecting the role that bodies such as volunteering organisations, private companies, or the military would play in crisis management.

Another key factor that affects the relevancy of collaboration is how risk is defined and how different incidents and hazards are characterised. For example, depending on whether an incident will be characterised as a 'major incident', 'a serious emergency' or 'a catastrophic emergency', the response might take a different shape and the collaborating stakeholders might change.

This means that when creating a CIS, it is important to see beyond the obvious first responders and consider what other stakeholders could play a key role in the management of the event. Similarly, a CIS should be set up in ways that support a variety of different direct users, beyond the core responders, at the discretion of the respective lead



organisation, and support a tailoring of the kind of engagement the CIS facilitates for these actors and parties.

Example

During the Prestige Oil Spill in Spain in 2003, the national government had not written plans in advance of the situation and the coastal communities could not have managed the clean up on their own. This meant that the local businesses and international NGOs had to play a major role in the strategic planning, decision-making, and the physical response.

From the start of the crisis, NGOs (especially the WWF) gave advice to the government and helped to coordinate the cleanup. The WWF created a crisis group to oversee communication and conservation policy strategies that involved various national organizations, holding meetings with government officials, scientists, national and local NGOs, local fishermen's organizations, and the International Tanker Owners Pollution Federation (ITOPF). In other cases, NGOs like the International Fund for Animal Welfare sent in emergency relief teams for animal rehabilitation centres and to train regional authorities and volunteers to collect, rehabilitate and release wildlife.

Academics from regional universities also stepped up helping to pool their data resources used in their research and to design a system that brought together the various data and actors for decision-making and planning purposes.

Tags: Inclusiveness, Diversity, Trust, Adaptability

Resources

Anderson, A. and Marhadour, A. (2007). Slick PR? The Media Politics of the Prestige Oil Spill. *Science Communication*, 29(1), pp.96–115.

Bossong, R., & Hegemann, H. (2015). Cooperation under Diversity? Exploring cultural and institutional diversity in European Civil Security Governance. In R. Bossong & H. Hegemann (Eds.), *2015 European Civil Security Governance, Diversity and Cooperation*. London: Palgrave MacMillan.

Garcia, R. (2003). The Prestige: one year on, a continuing disaster. *World Wildlife Fund*. Available at: <https://wwf.fi/mediabank/1085.pdf>.

Kuipers, S., Boin, A., Bossong, R., & Hegemann, H. (2015). Building Joint Crisis Management Capacity ? Comparing Civil Security Systems in 22 European Countries, 6(1), 1–21.

Petersen, K et al (2014) Overview of disaster events, crisis management models and stakeholders. SecInCoRe EU Deliverable. <http://www.secincore.eu/publications/deliverables/>

UNISDR. *Sendai Framework for Disaster Risk Reduction*. United Nations Office for Disaster Risk Reduction, 2015. Accessed 4 January, 2016. <http://www.unisdr.org/we/coordinate/sendai-framework>.

5.2.5 Protecting the Rights of Data Subjects

Hint: Protecting victims, responders and volunteers from data abuse

The persons whose data is being processed, so-called data subjects (victims, first responders, volunteers), have a number of specific rights. The architecture of any CIS



should foresee the exercise of these distinctive rights and accommodate the increased control of data subjects. The EU's General Data Protection Regulation significantly increased the rights of data subjects. This reflected a move towards increased end user control and "ownership" of their data and its use. As a starting point, there is a strong emphasis on transparency in relation to how data subjects' data is collected and processed. Any information on this needs to be intelligible, clear and easily accessible. Building upon this, there are a number of specific rights that the data controller must ensure can be met, usually within one month of a request being made. These include a right to relevant information about the controller and the processing of the information; a right of access to data, including information about the period for which the data will be stored; a right of rectification in relation to inaccurate or incomplete data; a right of erasure of data that is no longer required for its original purpose; and a right to data portability which relies heavily on data being recorded in an accepted standard to maintain interoperability.

Guiding Questions

Have you accessed and understood the rights available to data subjects in the GDPR?

Have you reviewed your provision of information to end users to ensure not only that it covers all required issues but also that it is written clearly and promotes transparency?

Have you developed policies to ensure that these rights can be supported within your system; pre-empting any requests by data subjects will enable the duties to be met in a much more efficient manner than acting retrospectively?

Who are the data subjects invoked in your CIS?

How are data subjects informed of their rights from the management/host perspective?

What about the rights of the users whose data is being logged?

Further Information

More in particular, data subjects have the following rights:

- The right to be informed in a transparent way about their data being processed (Art. 39, 60). This obligation is especially important vis-à-vis first responder agency employees. Victims might not have to be informed since it would require a disproportionate effort to do so during a crisis situation (Recital 62 and Art. 14§5 GDPR).
- The right to access the personal information that is being processed on him or her (Art. 39, 59, 63). By virtue of this right any data subject is entitled to ask a data controller whether or not information personal data concerning him are being processed and obtain information relating to the purpose, the recipients, the duration of the processing, etc.
- The right to rectification: Data subjects will have the right to request a rectification of inaccurate data concerning him or her (Art. 59).
- The right to erasure: Under certain conditions a data subject may require a data controller to delete data concerning him or her. This right would be enforceable for example in case of: unlawful processing, withdrawal of consent or when the data are no longer necessary for the purposes for which they were collected originally (Art. 39, 59, 66, 68).

For these rights to be exercisable it is of utmost importance that both data controllers and data processors maintain records of their processing activities and that they foresee standardised procedures that enable data subjects to exercise their rights effectively. The



exercise of such rights might require intense communication between the different connected entities which underlines the need for a common and predetermined procedures.

Example

Consider a victim during an earthquake. First responder agents take a picture of the victim to show an injury to a medical service and the next day this picture becomes visible on their website. In such a case it is obvious that the victim's data have been processed beyond the original purpose they were collected for. Since the data are no longer necessary within the context of the disaster relief operation, the data subject can request the erasure of this picture. In practice the data subject will address one of the data controllers participating in the CIS to exercise their right. Nevertheless, all of the entities connected to the CIS should make sure that they all erase any copy of this picture.

Tags: Proportionality, Privacy, Transparency, Respect, Trust, Justice, Data Protection, Informational self-determination

Resources

European Parliament and Council (2017) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Information Commissioner's Office (2017) *Overview of the General Data Protection Regulation (GDPR)*. Available at: <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr>.

5.3 Summary

This Chapter has described the 'Guidance' component of the ELSI Guidance and provided a listing of all Guidance as up-to-date on 26 April 2017. The current listing is evolving and available at www.islTethical.eu. The way in which the Guidance relate to ELSI that arise concretely addressed in specific guidance entries as links to Key Terms, described in Chapter 4 above.



6 Community Engagement

The Key Terms and Guidance have been developed predominantly for ICT managers who will make choices about CIS technologies and organizational innovation, including organizational practices of interoperability. They may, for example, turn to the Guidance during IT strategy planning, prior to procurement of an existing system, when implementing new or existing infrastructures, or when working with emergency responders as they develop training and exercises. They are also for those involved in governing or hosting such systems. Designers and technology developers, as well as individual users of a CIS may also find the Guidance useful in thinking about their approaches and choices when working with collaborative disaster IT. IT is also available to support transparency and public discourse on the use of CIS for DRM. It is publicly viewable at www.isITethical.eu.

6.1 *Isitethical.eu*

Bringing together work from a number of EU projects, including EPISECC, SECTOR and REDIRNET, the work has been developed into an open public platform hosted by the Public Safety Communications Network. This incorporates

- a functioning platform with critical mass core content and mechanisms for contribution,
- a concept for allowing this to evolve as a community resource.

Our approach is inspired by the U.S. Department of Health & Human Services' Research-Based Web Design & Usability Guidelines (<http://guidelines.usability.gov>).

6.1.1 The interactive platform

The platform is still under development. This section describes its status on 7th April 2017. The evolving and current version is available at www.isITethical.eu (Figure 2).

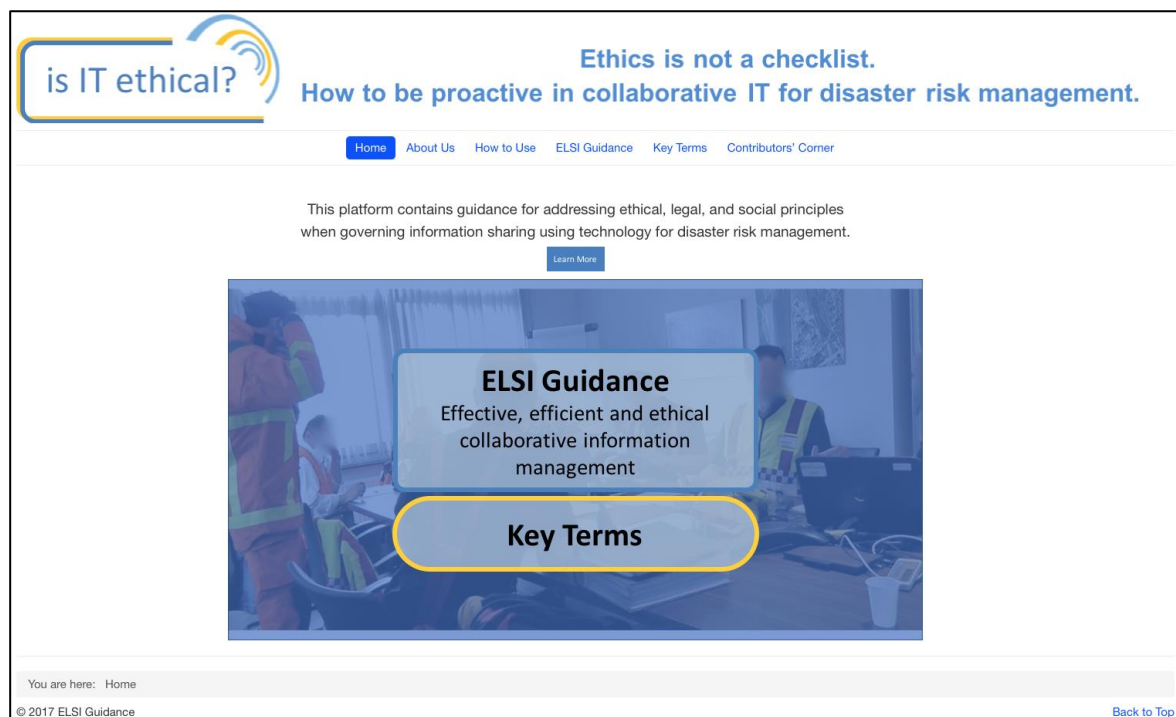


Figure 2 The ELSI Guidance Front Page



As users enter www.isitethical.eu, they are given the option to explore ELSI Key Terms or Guidance entries. The two sections are interlinked throughout the website. The Guidance supports users approaching the resource by asking practice-relevant questions such as “how can I initiate a collaborative CIS in a way that avoids building silos?”. The Key Terms section is a starting place for users who might have encountered particular issues, such as ‘partnership’ issues or ‘disclosure’ issues. Each section provides links to relevant guidance or terms.

When navigating to the Guidance page, a short explanation gives an overview of what is included here and the intention of the guidance (Figure 3).

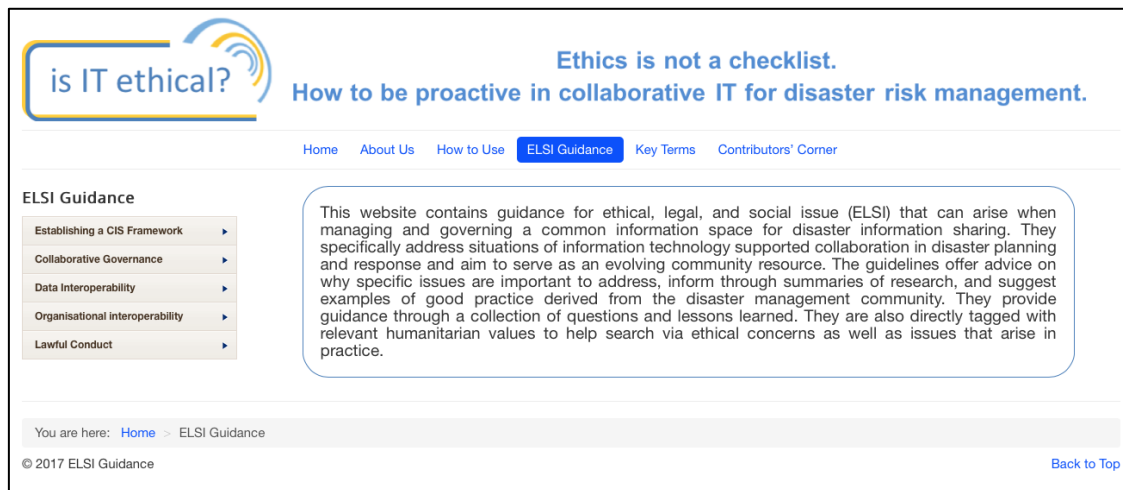


Figure 3 The ELSI Guidance landing page

The guidance component is separated into 5 chapters, each covering different aspects of collaborative IT practice: initial considerations before getting started, governance, data interoperability, organisational interoperability, and legal considerations. Users can select from a menu to explore the various guidance within each chapter (

Figure 4).

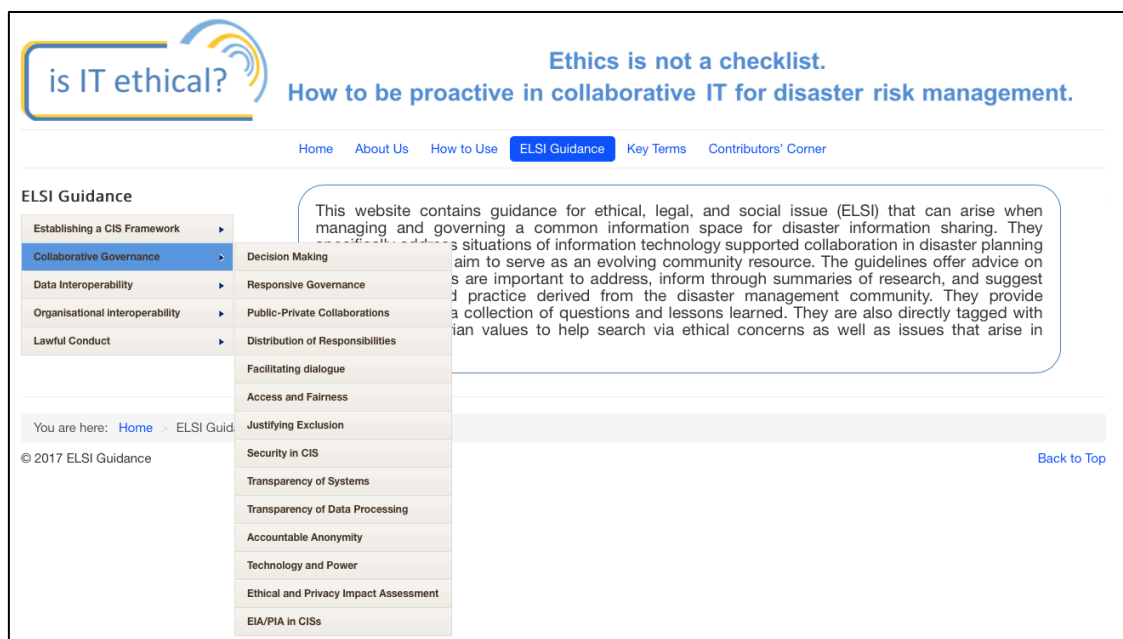
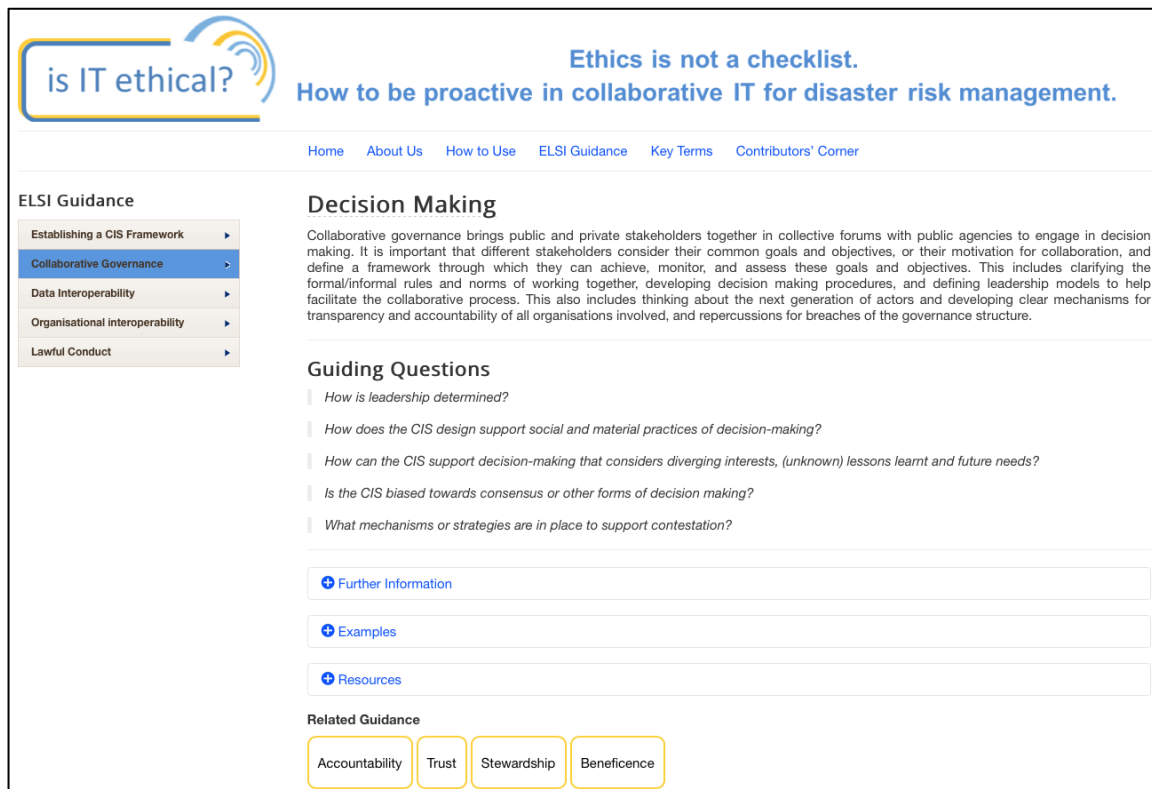


Figure 4 Guidance menu example

Once a guidance page is selected, a paragraph describing the issue at hand explains key dimensions. This is followed by some guiding reflexive questions that have no single correct answer, but can help address the ELSI that could arise (Figure 5). More detailed investigation of the issues can be revealed by clicking on the 'Further information' tab to expand that content, augmented by similar 'Examples' and 'Resources' tabs. Also, links to related ELSI Key Terms are provided along with each entry. These links allow users to understand how this issue connects to wider and often interconnected ELSI, and it also allows for a more detailed exploration down a single path. If, as in Figure 5, for example, a person was interested in considering digital divides as an equality issue, they could follow the link to equality in order to explore that aspect. Associated with that Key Term, they would find other ELSI Guidance, exploring other areas where equality has been found to be an issue. This is intended to enable broader ranging, in-depth, consideration of issues.



is IT ethical? Ethics is not a checklist.
How to be proactive in collaborative IT for disaster risk management.

Home About Us How to Use ELSI Guidance Key Terms Contributors' Corner

ELSI Guidance

- Establishing a CIS Framework
- Collaborative Governance**
- Data Interoperability
- Organisational interoperability
- Lawful Conduct

Decision Making

Collaborative governance brings public and private stakeholders together in collective forums with public agencies to engage in decision making. It is important that different stakeholders consider their common goals and objectives, or their motivation for collaboration, and define a framework through which they can achieve, monitor, and assess these goals and objectives. This includes clarifying the formal/informal rules and norms of working together, developing decision making procedures, and defining leadership models to help facilitate the collaborative process. This also includes thinking about the next generation of actors and developing clear mechanisms for transparency and accountability of all organisations involved, and repercussions for breaches of the governance structure.

Guiding Questions

- How is leadership determined?
- How does the CIS design support social and material practices of decision-making?
- How can the CIS support decision-making that considers diverging interests, (unknown) lessons learnt and future needs?
- Is the CIS biased towards consensus or other forms of decision making?
- What mechanisms or strategies are in place to support contestation?

[Further Information](#)

[Examples](#)

[Resources](#)

Related Guidance

Accountability Trust Stewardship Beneficence

Figure 5 Example Guidance

The reverse is true for users starting from the Key Terms, where a landing page, once again, provides a general explanation of the content in this section and the intention behind this, as well as a list of Key Terms to navigate to (Figure 6). When users explore individual Key Terms, they find a short explanation and a list of key aspects to consider. This provides a quick overview and some direction. The aspects listed as bullet points suggest goals that should be achieved in and through collaborative disaster IT. Each page then links to related guidance pages that offer insights and reflexive questions as to how to potentially achieve those 'shoulds' (Figure 7).

As it is intended to be a living community resource, meant to support reflexivity around ELSI as well as grow and expand based on the experience of those that use it, the site is supported by a 'Contributors' Corner' (Figure 8), which invites users to comment, or provide



concrete suggestions for the inclusion of new guidance entries, key terms, examples, further information or resources.

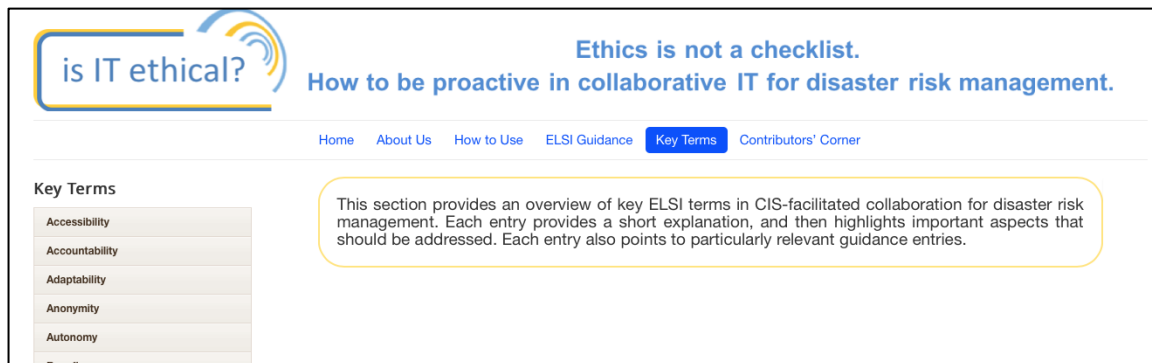


Figure 6 ELSI Key Terms landing page (excerpt)

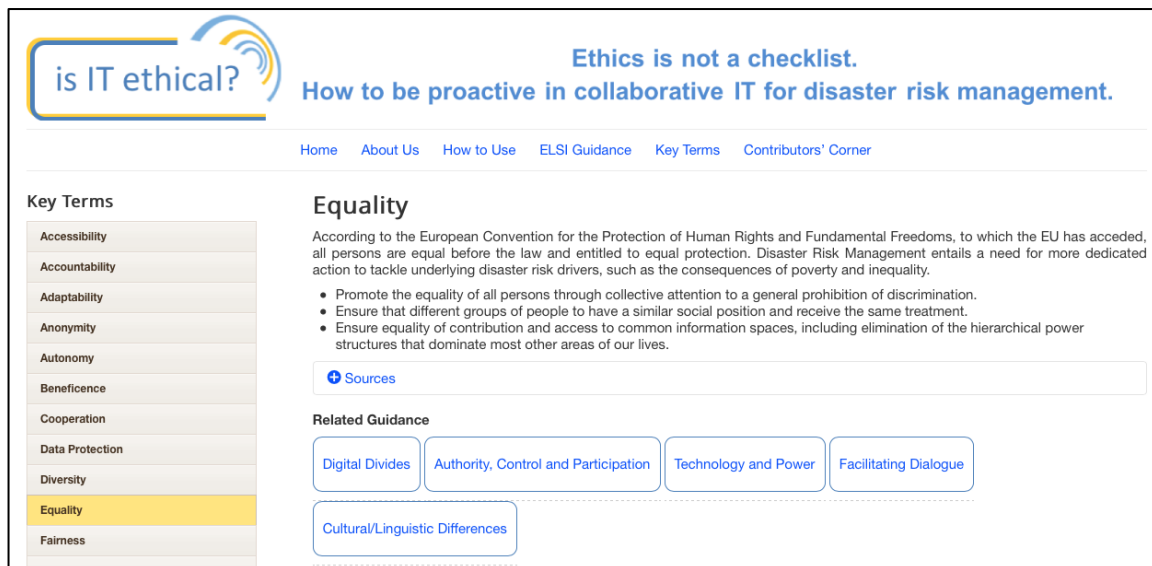


Figure 7 Specific ELSI Key Term

6.1.2 Governance of the Community Platform

The ELSI Guidance brings together diverse perspectives on, as well as experiences and practices of, innovation in collaborative ICT for DRM. It is critical to note that the Guidance that results from this collaboration are not a product but a process in nature. While we have developed a core of content and structure, what is presented here is intended to support an evolving process of producing, enriching and utilising the Guidance as a community service. The governance structure is designed to aid constant modification, learning, and growth.

The ambition of making the guidelines live, lived and living was also fulfilled through making the process of producing this initial product participatory and inclusive. A strategy of 'collaborative experimentation' was pursued that provided multiple channels, from workshop discussions to practical applications of drafts, for engaging in the design and use of these guidelines. Isitethical.eu is set up ideally to continue this interactive process.

There is a recursive relationship between ELSI and technology (see, for example, Hoven & Weckert, 2008). Practical knowledge and moral principles are culturally specific, subject to contestation, and shift in times of disaster. Thus, in order for Guidance to be useable, they



must be transparent in regards to their cultural positioning, be flexible enough to be adapted to other contexts, and be open to debate and change.

Figure 8 ELSI Guidance 'Contributors' Corner'

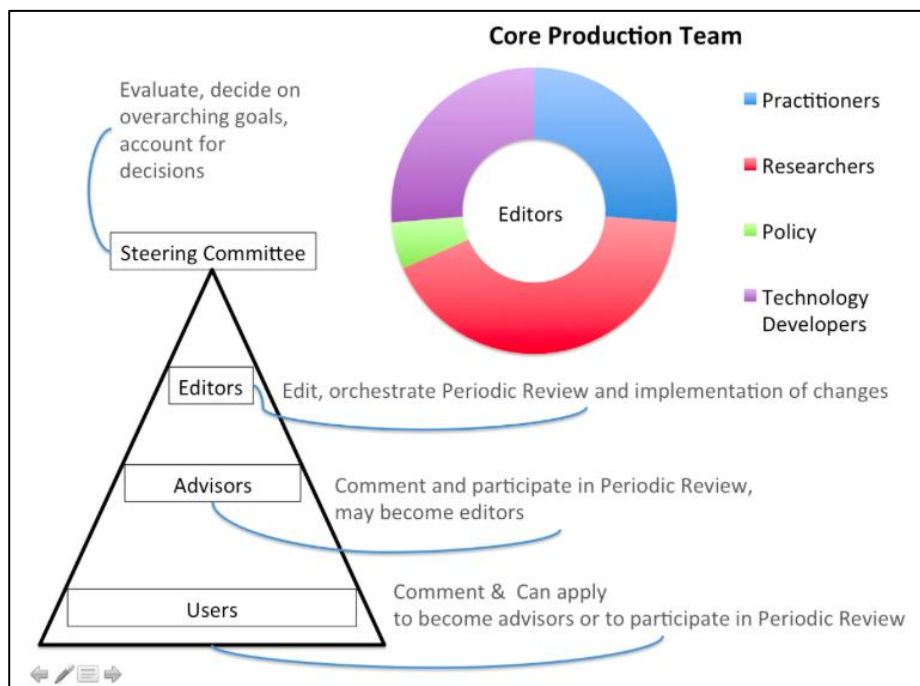


Figure 9 ELSI Guidelines Governance

An advisory board governance structure is being implemented (see Chapter 9 on Future Work). The overall purpose for the open governance structure and process-oriented design of the platform is to ensure that 1) the Guidance and Key Terms address the ever-changing



realities in digitally augmented collaborative DRM and 2) to draw on expert knowledge from practice.

6.2 Playful Offline Interaction

A range of activities embed the online Guidance platform at www.isitethical.eu in wider societal contexts and DRM practice. This includes offline collaborative experiences. One of those is a multi-player board game, in which users work through ELSI as they work together to set up a CIS for responding to specific disasters.

The research underpinning the Guidance is a form of design research (Frayling 1994, Büscher et al 2011), which utilises creative processes to deepen the impact and contextual sensitivity of the work undertaken. To this end, an Isitethical board game has been developed that also draws on future orientated design approaches such as Design Fiction, Critical Design (Dunne 2008), and Speculative Design (Coulton et al 2016) and game design practices such as Critical Play (Flanagan 2009), Persuasive Games and Procedural Rhetoric (Bogost 2007). The game has two main objectives. Firstly, it aims to create an off-line form of engagement with the Guidance that allows stakeholders to playfully explore alternative realities of digitally augmented DRM and plausible futures (Coulton et al 2016), with transformative consequences for the actual present realities of DRM and possible futures. Secondly, the aim has been to create a framework that allows users to experiment with ethical impact assessment as a collaborative creative process.

From the starting assumptions that past and present are individually constructed to create particular realities (Law and Urry 2004) or rhetorics about reality, and that design can be considered “as rhetoric” (Buchanan 1985), we designed a game with the premise that each time it is played worlds are built, and in these worlds players can experience the ELSI Key Terms and Guidance ‘live’ – in effect playfully ‘living’ them. This gives a different ‘lived’ perspective on present experiences and imaginaries of futures. Persuasive games are defined by Bogost as providing an alternative approach, one grounded in utilising rhetoric to reveal to the player the underlying processes or concepts that drive a system or activity through playing the game (Bogost 2007) in our case this concerns appreciation of the complexities and critical reflection on ethical legal and social issues and socio-technical practices in the context of emergency response.

Game worlds have much to offer in relating complex concepts to players as they allow them to revert causality and replay scenarios. Game worlds create playful, subversive and irreverent spaces, often described as the ‘magic circle’ (Salen and Zimmerman 2004) that allow players to critically explore serious issues of the real world. Game design and speculative design may result in artefacts that can also often appear subversive and irreverent in nature (Coulton et al. 2016), however they can be effective tools to instigate conversations and creative thinking on complex issues otherwise too difficult to approach, especially in a context of conflicting perspectives.



Figure 10 The ELSI Guidance Game

The design of the game started from the principle that ELSI Key Terms and Guidance should support practice. The game builds worlds in which players engage in practice with challenges and opportunities of emergency responders' socio-technical practices. The game is a collaborative experiment that instigates ELSI reflexivity and supports creative thinking in the context of complexity.

Each individual ELSI Guidance has emerged from examples built upon past incidents, drawn in part from SecInCoRe's past disaster inventory, in which the issue arose, the game then aims to put the research examples in motion to create situations in which ELSI guidance gets debated, used, evaluated. In this sense, the game is also a way to catalyse community building and tangible ways to support engagement with the online IsITethical resource. By playing, the aim is to facilitate encounters, instigate conversation and discussions of the ELSI key terms and guidance beyond a website. The board game ultimately makes SecInCore findings engage-able and appealing to wider audiences including other practitioners that are considering in ELSI in other contexts.

6.2.1 Elements of the game

It is cooperative game. Players are against the mechanics of the game, aiming to 'beat' the game. Cooperation within the game is neither straightforward nor explicit, and there is a great temptation to act solo, especially for first-time players. However, a crucial moment in the game, is when players realise that the best way throughout is joining forces and working together. Working together is not simple. Players have to overcome inter-organisation rules and codes, technological challenges, and clashing responsibilities.

It aims to produce an endless narrative. Each time that it is played, the game combines the stakeholders' individual goals (set specifically for each hand) with the overall goals of the organisation to which they belong (e.g. police force, transport operator, environmental agency, utilities service providers, etc.) and the goals set in the CIS that they host and operate. Each combination creates a different setting every time the game is played and therefore the ELSI Key Terms and Guidance can be discussed in a range of different situations, locations and types of emergency (chemical spill, natural disaster, medical epidemic and terrorism). Each stakeholder's possible action is also dependant of the relation



to the others players or stakeholders, also to each others' capabilities, possibilities to share data effectively and access to technology and resources.

Another important element of the game is that it represents some of the hazards as responsibilities. All the actors in the game are not just responding to hazards or managing risks that appear by chance but are direct consequences of their actions.

It aims to instigate cross-culture (countries and organisations) collaboration. The game represents the tensions of public and private stakeholders, of responders with international capacities and local or regional responders, and opportunities and challenges that participation of social media and volunteers stakeholders may offers in an emergency response scenario.

Players will engage in designing, hosting, governing, and operating a CIS. A central aspect of the game is the construction and governance of secure, dynamic cloud based knowledge and communication system CIS. The player, as host of or stakeholder within a CIS, gets immersed in decision-making processes, experiencing through play the advantages and costs of that CIS. The game offers opportunities for players to be reflexive and proactive about opportunities and challenges in collaborative work practices such as information politics, organizational culture, technology dependence, data protection, digital divides, and social sorting.

The game offers a world in which to experience situational discussions and debate of ELSI Guidance. In the world of the game each ELSI is an action, sometimes implying discussion and decision-making, with negative and positive effects. In other situations an ELSI can facilitate a better cross-border, cross-institution strategy. With this, the game highlights ELSI as part of and emergent from practices and technologies, not just abstract values that need to be achieved. The player should never experience ELSI as a policing force, but as a collaborative practice that instigates critical reflection and decision-making that involves working with individual and collective goals, resources, and technologies.

Part of the task of designing the game was to represent data collection, storage, exchange, and understanding. Representing the formalization of the emergency response context including obstacles of data reuse, data interoperability and data access. Also, the mechanics of the game highlights obstacles and problems, not just ethical, social and legal, but also in terms of capacity to respond if too much data is collected or obstacles of data managing when data is repurposed or separated from its context, or removed from the interests that informed its collection. In doing so, the game intends to tangibly represent the mobility of information, resources, and people in a combination of digital and physical that can be hard to otherwise visualise.

The first prototype of the game has been piloted in four different contexts. Tests have been conducted in the Centre for Mobilities Research, in Imagination Lancaster open studio, with a class of first year Design Interaction students at Lancaster University, and with a group of young teenagers (football players of the local community). In the four occasions the game extended beyond the end of play into conversations, proving that the game – like many training exercises – is more than what happens at the table, and is an excellent initiator or meaningful interactions with the ELSI inventory and guidelines. The next iteration of the game design will be tested with emergency responders.

6.3 Rethinking the EIA

ELSI are often treated as if outside of the longer-term design process, as if they are something that can be externally checked on occasion to make sure innovation is on the right track. Doing so, has led to a common practice within socio-technical innovation for those engaged in considering ELSI to have to learn a great deal about technology, design,



and general innovation practices, while those engaged in the more technical aspects have to learn very little about either the social sciences and humanities research or the wider societal practices within which their designs will be engaged (Balmer et al 2016; Viseu 2015).

Instead what is needed is collaborative experiments between the social sciences and technology in ways that the result of these collaborations is the ELSI themselves. The Inventory and Guidance are one piece of this larger project of rethinking the ethical impact assessments (EIA). The aim is to find ways of moving EIAs away from processes of external expert evaluation to include processes of collaborative reflection and mutual learning (Petersen et al. 2016). This shift in approach to EIAs can move them beyond raising awareness about an ELSI laden situation or acting as a test for 'wrong' technical solutions, to providing tools for reflexive inquiry into what might be the best solution for a given situation or an unforeseen social-technical blueprint for action.

The aim of an EIA is to provide tools to examine the ethical issues surrounding the design, use and social impact of technology. This includes how values are imbedded within a technology. A variety of approaches exist that:

- Typically emphasise the importance of procedurally identifying ethical issues and involving stakeholders in the process (Wright 2011).
- Often these focus on end-user needs, values, and desires (Friedman et al. 2013).

This includes ethical issues surrounding the “design, use and social impact of technology” (Verbeek 2011, p.3) as well as the study of the technology itself, including its “embedded values” (Nissenbaum 1998) and morally opaque features (Brey 2004).

But a shift in EIA aims to expand it to also:

- *Make ELSI concrete*: To think with reference to specific case studies so that our design and concepts might help notice and address ELSI. One way to do this is to emphasize societal concerns (not just end user needs) and the broader socio-technical context of use (Yoo et al 2013).
- *Deeper dialog*: Engage in multi-disciplinary inquiry that includes emergency response practitioners, social scientists, engineers, and IT designers. EIAs, from this perspective, should help develop “infrastructures” to support “collective inquiry into matters of concern” (DiSalvo et al. (2014, p. 2403).
- *ELSI aware innovation*: To bring attention to how ELSI are emergent within design and situated use. This requires a move away from treating design and use as separate phases (e.g. Schot and Rip, 1997).

By contextualizing ELSI in these broader frames of matters of concerns and infrastructures, EIAs can be conducted so as to develop ways to support deliberation that provide richer understandings of how ethical issues could be addressed. As Bodker states: “designers get more of a feel for the potentials and problems of their future artefact in context, and thus really understand the problems as well as their current solution better” (Bodker, 2000, p. 73). And, as Carroll writes, such a broader, more contextual and situated frame, can evoke “action-orientated reflection” about different design moves and diverse user practices – as opposed to cleanly delimited “user needs” (Carroll, 2000, p. 50). In other words, by moving away from the designer/user dichotomy to a societal context and situation of use frame, ethical, legal, and social problems become dynamic.

The need for such shifts in how EIAs work and the reflexivity of EIAs can become evident throughout SecInCoRe’s EIA process. Even when specific issues were focused on, such as privacy or trust, it became clear that without this new framing, these ELSI were engaged with



as states of being. Either privacy is maintained or it is not. Either people trust or they do not. Such considerations could be called 'ELSI by design' (inspired by ideas on 'privacy by design' (Cavoukian, 2001)).

But discussions through specific case studies, for instance, revealed that roles and interpretations of data protection laws change (over time and over borders). For example, exploring SecInCoRe's innovative potential through a case study of the Germanwings crash made clear that German conceptions of privacy are not the same as French or British. Or, when discussing trust it was evident that if data seems irrelevant or inconsistent, people will not trust it. But it emerged through these discussions that what might seem normal or irrelevant in isolation or abstraction can tell a different, specific, necessary story when seen in context. It quickly became clear that there were no certain "rules" on this issue to embed in the technology or provide clear rules for design, especially in regards to a pan-European technology (Petersen et al 2016).

Within this same case-study based EIA, the co-pilot's previous flight records which had been seen as normal, but now, in context of the crash and his medical and internet search records, seem like test-runs for the crash. Before the crash, we trusted the system that isolated and reprioritised the flight records. That's no longer the case. Trust is *made*, it is not a state (Clarke, Hardstone, Rouncefield and Sommerville, 2006). As these issues were explored, this shift in EIA frame also revealed a disconnect between the questions (about user practices with data) and the answers (about system security). It made it possible to ask different types of questions: what makes trustworthiness? Accuracy? Consistency? Previous Experience? Completeness? Comparability? Security? The discussions turned from a check box of whether data is trusted or not, to how to map relationships between data, technological practices, and ethical issues and design in ways that consider those maps (Petersen et al 2016). How you ask questions about trust can change a whole design trajectory, not just if this solution will be trusted or not.

ELSI cannot be treated as isolated phases within design (isolated from conceptualization, design, governance, and use), but as an interdependent component of a larger disaster IT practice. The potential benefits include:

- grounding collaborative reflection and learning in the ambiguities of real world experience
- connecting complexities of practice with complexities of design through concrete narratives,
- opening debates around situated use of technologies to facilitate the development of creative strategies and responses.

This process can also help those conducting EIAs to see the limitations of their knowledge and experience and identify where we need to engage further with practitioners (Petersen et al 2016).

Equally, important, however, in rethinking the EIA, is about social scientists and humanities researchers letting go of the idea that ELSI belongs or is owned by the them and so that it's the social scientists' onus to labour/carve a space for their brain-child in the inhospitable environment of the technologist's realm. Instead a double move needs to happen. The social scientists need to let go and the technologists need to step up (and be counted). The disciplinary boundaries and harnesses need to be let loose on both sides. We need to carve collaborative experimental spaces where we can allow for the ELSI to emerge as 'issues' that manifest themselves exactly on those liminal collaborative spaces where no one can claim ownership yet everyone is deeply implicated. This also means 'staying with the trouble' and working 'in the belly of the beast' instead of moving away from it (Balka 2006).



7 Implementation of ELSI Guidance within the SecInCoRe project

As SecInCoRe designed a proof-of-concept Common Information Space for pan-European disaster interoperability, it not only developed the concept of the ELSI Guidance, but also drew upon them to influence and inform the forms taken by the innovation and conceptual design. This chapter first offers an explanation of the main features of a Common Information Space upon which SecInCoRe focused. It then provides examples of the various ways in which ELSI emerged and the ELSI guidance was implemented within the reference implementation, user experience, or as part of the system governance.

These examples are not intended to be comprehensive to either the SecInCoRe project nor to how the ELSI Guidance can be implemented within collaborative disaster IT. Rather, they illustrate a range of approaches and tactics for working with this Guidance, including demonstrating how ELSI can be treated as integral to innovation -- as an ongoing social and technical process -- rather than an external check on design decisions.

7.1 Considering ELSI in Common Information Spaces

SecInCoRe provides a toolkit to support the establishment and implementation of a Common Information Space (CIS). CISs are powerful concepts that respond to needs for data sharing, collaborative sense-making, and coordination (Pottebaum et al 2016). They aim to support people in constructing a shared sense of a given situation without requiring everyone to have the same understanding, goals, or details. They are produced in and through collaboration practices, such as sharing data/information, cooperating, negotiation, discussion, finding new partners, and are enabled by digital and organisational infrastructures. Each CIS configuration and related needs are unique because how issues should be addressed depends strongly on the specifics of the situation in which they arise.

However, taking CISs from concept into use is proving disruptive, raising complex ELSI. While these new tools hold considerable potential, they also require the negotiation of a variety of perspectives, and they come with potential challenges to existing practices of establishing trust, legitimacy, privacy, and power. They can exacerbate internal politics between organisations, aggravate sensitive cultural problems, and interfere with the ability to support humanitarian values. As importantly, these issues also raise opportunities for more inclusive risk governance, enhanced security, and better ways of exercising solidarity (Büscher, Liegl, Rizza, & Watson 2014).

SecInCoRe found that in order for their CIS to be an effective environment that enables collaboration, coordination, and communication between different types of stakeholders -- including responders, the public, NGOs, and private actors -- it needs to support reflexive practice and attention to the ELSI that arise in their design, implementation, governance, and use. Working with the ELSI Guidance, SecInCoRe established some techniques within its demonstrator for raising awareness of possible ELSI (e.g. when data protection issues might arise).

7.2 How ELSI translated into SecInCoRe

SecInCoRe's CIS is intended to take a range of shapes (depending on existing tools, practices, and needs), to address various scales of activity (from supporting local cross-agency interoperability to pan-European information sharing) and to support productive interactions between diverse and potentially new stakeholders. Throughout the collaborative design process, it became evident that it was necessary to design the CIS in a way that supports practices of inclusiveness, to help people see each other's relevance and avoid further silo-ing, while still being able to justify exclusion and autonomy. To illustrate how the ELSI Guidance supports CISs, below are solutions derived from engaging with the Guidance within components of SecInCoRe's modular CIS demonstrator.

7.2.1 Knowledge Base/Inventory

The Knowledge Base is a growing inventory of data sets, documents, case studies, and meta-data that can be added to within CISs and searched using the Semantic Search. It is similar to any general database, but structured in a way that is domain specific and thus with categories and interrelationships that are more relevant to DRM. But databases carry with them the cultural and organisational logics of those that design them, leading to potential ELSI, including leading to **mission creep** or creating unexpected barriers for **inclusiveness**, **fairness**, long term **stewardship** due to being forced to work within a different system of analysis than one's own.

Guidance Consulted: Contextual Reasoning

How are participants encouraged to provide background to their data?

What are the mechanisms? What background is needed?

The CIS needs to provide contextual understanding of why specific decisions were made, why an incident played out as it did, why and how the data was gathered and towards what goals. This can mitigate inappropriate uses of data and promote finding data from new sources that can be deemed valuable in new and productive ways.

- To ensure no single source or perspective becomes authoritative, within the governance of the Knowledge Base are instructions that all case studies come from a range of sources.
- Inclusion of ELSI and lessons learned categories within the case studies to support the users identify and gather next steps for future incidents (Figure 11).
- After uploading a document, keywords can be accepted or edited by users that act as meta-data that can be used to provide details about the document's purpose and initial goals.

Search	Graph	DB Details	Edit
media	National and Regional Media Emergency Forum network and Media Centre were established during the morning. This structure had been in place since 2001 and was a reaction to the 9/11 incident. Initial updates to avoid travelling were sent out quickly and correctly, although subsequent information was not used as effectively. The media were still using some out of date information later on the 7th. Initial updates given by the Metropolitan Police Commissioner, although this caused confusion later on when junior officers took over and their reports and comments were not seen as carrying the same weight. Agreed at the debrief that media should be part of major incident exercises but that there is a difficult relationship between the use of the media to warn and inform the public for safety purposes and the media role to report and interpret what it sees.		
elsi	Racial Stereotyping: In the immediate aftermath of the bombings and despite strong condemnation of the incidents by Muslim leaders across Europe, there were some racially motivated and anti-Muslim attacks. Mythologizing places and extremism: As a result of events both before and after July 2005, it was argued that Luton, the town where the 7/7 bombers joined the train to travel into London had become synonymous with Islamic extremism and racial tension (Travis 2006). Personal Privacy: The police took over 12,500 statements from witnesses; acquired 26,000 exhibits; seized 142 computers and obtained more than 6000 hours of CCTV footage for evidential purposes and / or forensic examination (EUMC 2005).		
dataSets_used_gathered_prior	Hard copy and computer-based mapping systems London Underground network systems (TrackerNet)		

Figure 11 Screenshot of past disaster case studies within the Knowledge Base, showing (centre) the ELSI that emerged

Guidance Consulted: Justifying Exclusion

What are the motivations and benefits of excluding a stakeholder from the CIS?

Do they outweigh the disadvantages?

It was clear throughout SecInCoRe's research that blanket sharing and access to all information in a Knowledge Base by all groups with a CIS would be highly problematic because of the potential for compromised information and conflict. This could especially be the case when, for example, an electric company needs to be a part of the CIS because they are directly connected to flood planning yet also have private data they cannot, or do not want to, share with everyone. At the same time, it is important that the CIS is not set up in ways that routinely exclude potential stakeholders and local knowledge, since that could inscribe **discrimination** and **injustice**. In order to support the necessary limits in interaction and sharing necessary to build and maintain **trust** in each other and the system without perpetuating value imbalances, it was necessary to build in the ability to exclude architecturally, but also make **transparent** how and when these systems work.

- When uploading document, users have the ability to define various levels of access to documents and data, access levels that are visible to all.
- It is not only possible, but simple, to request access when it is denied (Figure 12).
- Document owners are able to change that access to their material for an individual or for all collaborators of a certain class.
- Meta-data for all documents are visible to all users, even if the document contents are not, so that all documents appear in search results and so that users have enough context to determine if they should request the restricted documents.

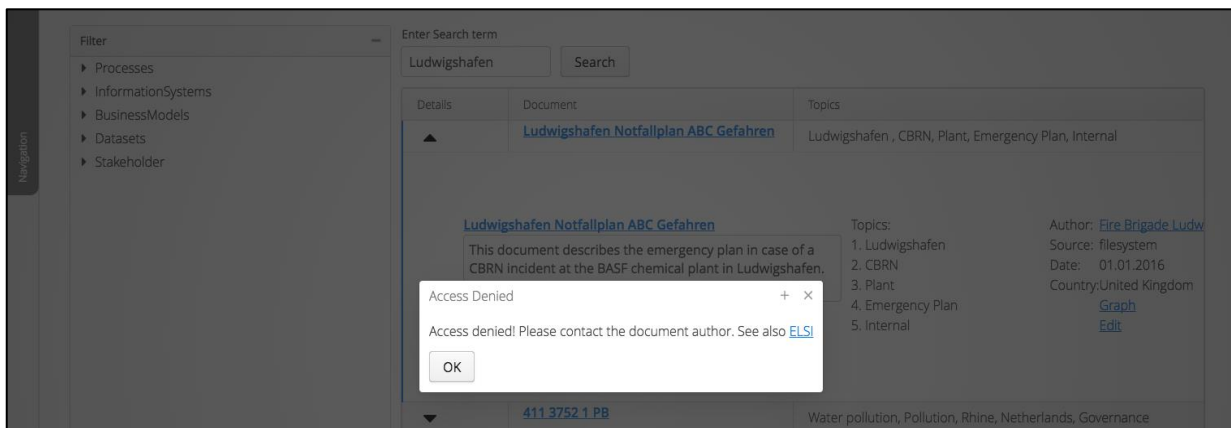


Figure 12 Screenshot of the access denied message that appears when trying to access a restricted document. The message also suggests contacting the author and visiting the ELSI Guidance for further explanation.

Guidance Consulted: Privacy and Personal Data Protection

When do I process personal data?

Because the legal concept of "processing" is very broad, referring to any kind of operation that is performed on personal data including, but not limited to: collection, storage, consultation, transmission, and erasure. Personal data is not the type of thing that can be guaranteed to be detected by a technological system, leading to potential breaches of **privacy**; questions about who was responsible for the **data protection** – the author, the



sharer, or the reader; or questions of anonymity can be broken because data is connected together.

- Organisations typically have data protection authorities that make sure shared information complies with regulation. When uploading a document to the Knowledge Base there is a link to guidance explaining why the document should have been through the local organisation's data protection authority. If they don't have a local authority they need to confer with the CIS governance/hosts structure before it can be uploaded (or refer to our guidance).

7.2.2 Semantic Search

Semantic searches, in general, provide different types of search results than the typical keyword/frequency algorithms. Built upon ontologies that provide contextual, domain-based meaning, the search results aim to speak to searcher intent, not just searcher word choice. Doing so makes it possible, for example, for a user to search via their local terminology but get results that connect to the related, but different, terminology of others about which they might be unaware. In such a **diverse** environment as a DRM CIS, however, the ontology will always be incomplete and will always need to be approached with **adaptability** in order to **respect** its specific user base in ways that support **collaboration** instead of **fragmentation**, and to avoid providing search results that seem irrelevant for lack of contextual knowledge or that guide searchers to specific, pre-defined, results that reinforce specific power structures.

Guidance Consulted: Transparency of Systems

How can inner logics and functionalities be made both visible and understandable, when needed, to those governing and using the technology?

SecInCoRe acknowledges that when the Semantic Search was designed, no matter how diverse the stakeholders consulted in its production, social logics are still programmed in. Making those logics as visible as possible for those wanting to implement the system was a necessary step in the design in order to not accidentally exclude or make invisible specific parts of social or political (or risks assessment) worlds. The challenge, however, was how to make these logics visible without overloading users with too many details.

- The ontology is visible and explorable within the search function itself, not just a logic that invisibly acts behind the search. This was done through the graph view as well as the menu of filters (Figure 13).

Figure 13 Screenshot of the search filters (left hand side) and the keyword/meta-data listing (grey box) that appears with each search result



Guidance Consulted: Configuring Awareness

How does the CIS support users in being aware of others?

How can users understand and control the flow and visibility of information within the CIS, including what is revealed, when, to whom?

Within a semantic search – and a CIS in general – users must understand where others' attention is directed in ways that make it possible to both intervene and encourage specific foci, shared lines of sight, and a general awareness of what each other are doing. Not everyone within a CIS needs to know what everyone else is doing in order to support this aspect of **cooperation** and **respect**, but it is important to understand how to point out useful information to someone else that might have been missed or to make it clear to others your goals so they can best provide the information you need in return.

- Collects user terminology, puts it in relation to each other through the taxonomy, and makes those relationships visible through the graph view search.
- Visualisation tool, highlighting how one's document is related to others (Figure 14).

Guidance Consulted: Multiple Perspectives

How can the system be set up to support the identification of intended concepts, terms, and technologies without forcing everyone to understand in the same way?

Because terms or roles across agencies or boundaries vary, for a semantic search to support **inclusiveness**, it should not require everyone to fit their data and communication patterns into a single organizational or classification scheme. But to do so it needs to create an awareness of how these different standards interrelate, not just through commonalities but also through what is unique to best know where to turn when seeking support.

- These relationships can be explored through the graph view in order to better see how different terms connect to gain insight in how to structure one's own searches to better find new material and how to structure one's own keywords to make their documents and data more visible to others in ways that demonstrates value (Figure 14).

Guidance Consulted: Producing Meta-Data

How can meta-data support a diversity of data practices?

A meta-data system was built that helped provide information about context of gathering, intended use, and risk analysis framework. This involves including within the document/system meta-data standards: the ability to access to information about author and contact information, and provide categories/data that provide enough context to support those who speak different languages to see value, usefulness, or irrelevance of a document without a full translation.

- With the keyword editing, link or pop-up to the "Producing Meta-data" and/or "Contextual Reasoning" Guidance.
- Translations of basic information into English.

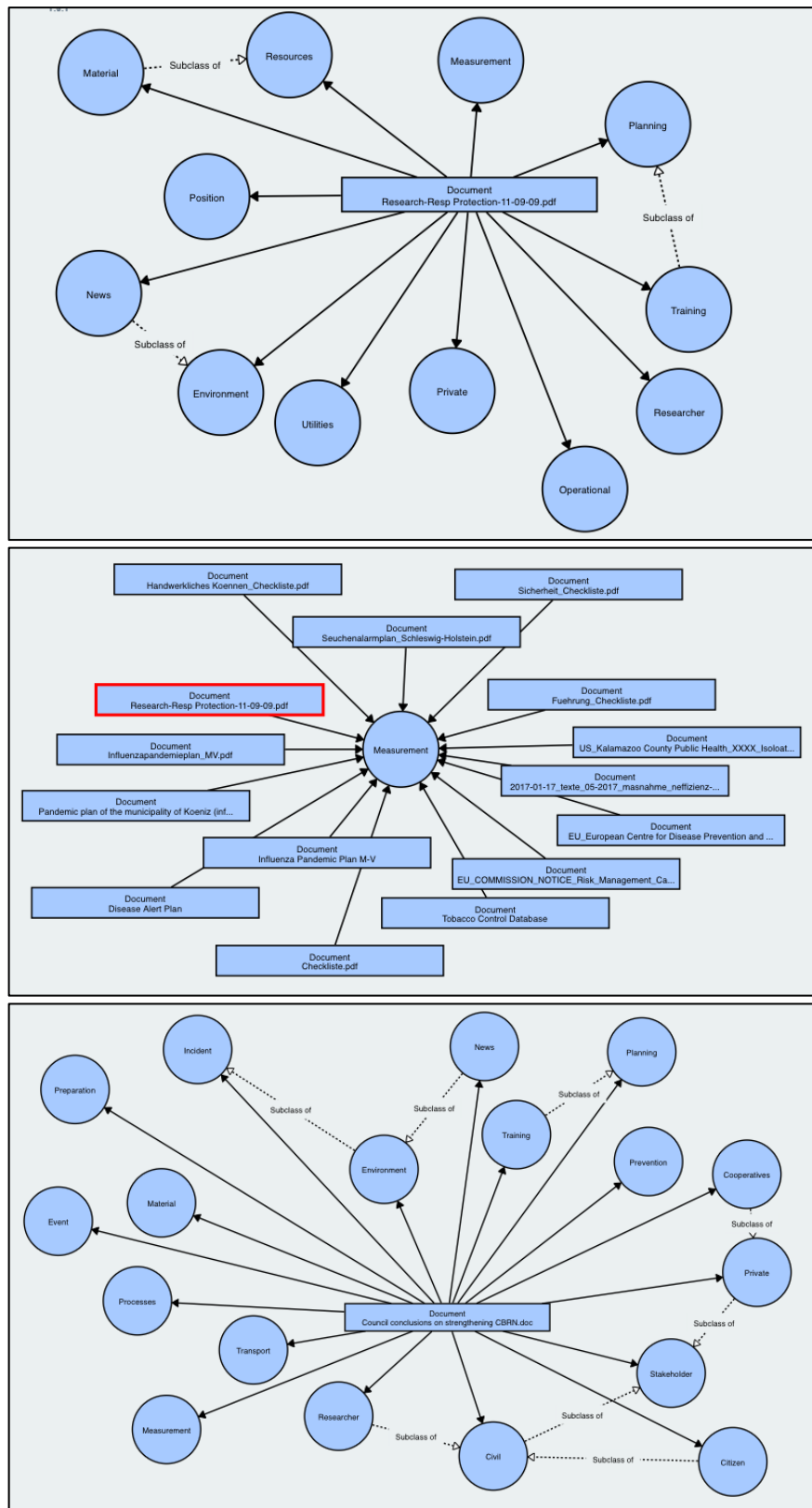


Figure 14 Screenshots of graph view search sequence, following the taxonomy to see interconnections: document with tags (top), click on tag to get related documents (middle), click on new document to get more tags (bottom)

Guidance Consulted: Articulation Work

How might it be possible for users to see relevant information to enable a cooperative working division of labour? Can this be done without information overload?

How might it be possible to be aware of other's actions, intentions, and activity flows within the CIS in order to support dovetailing?

Cooperating actors must coordinate and interrelate their respective activities as they engage with the keywords and graph view. The underlying ontology within the semantic search, being based in a mix of real-world semantics and domain specific taxonomies, is intended to provide sense of disciplinary context over time that can help users think about a bigger picture and new information within their personal familiar frame of action.

- The ability to edit document tags to better suggest why something was useful, not just describe the documents contents that can get generic when in large quantities (Figure 15).
- Support in seeing how others classify their own documents in relation to yours. Search for related documents via ontology that connects keyword patterns and provides related author contact information.

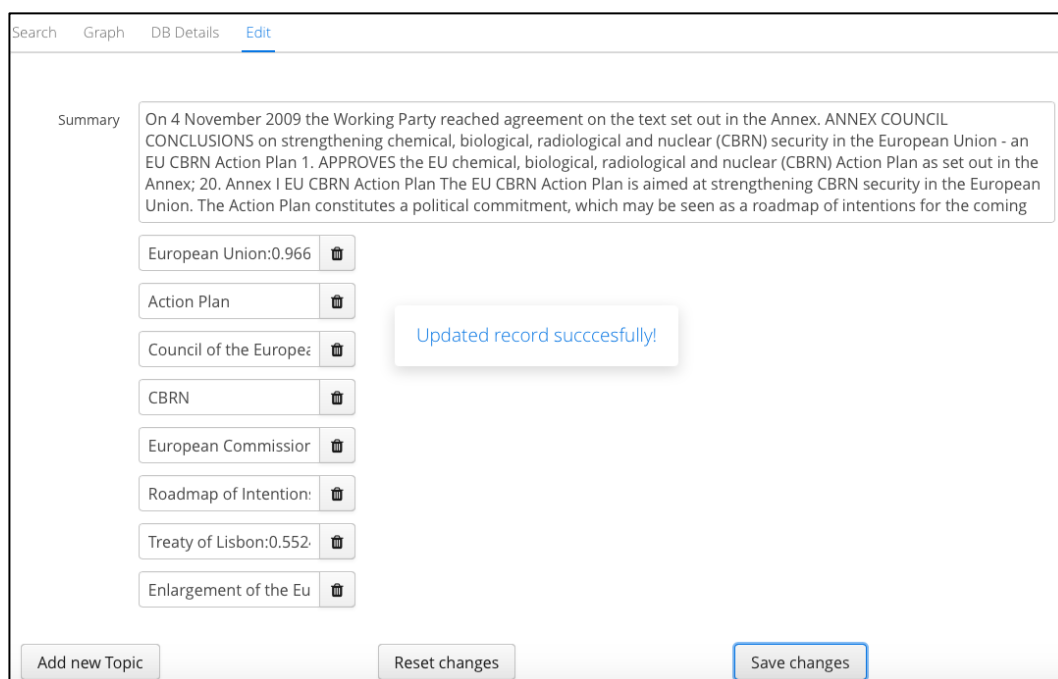


Figure 15 Screenshot of meta-data keyword editing

Guidance Consulted: Multiple Crisis Management Models

To what extent can the system be flexible enough to support change yet stable enough to be enacted cooperatively?

Design and practices both need to be built with flexibility and reversibility. Be flexible enough to not impose one community's way of thinking, doing, planning. Encourage in how interactions are set up a degree of reflexivity towards thinking about meaning of information (yours and others) for the different groups involved. One idea behind the Semantic Search was to have it be one step in making it possible for users to hold, in the same space,



conflicting ideas and to still be able to take action without assuming or expressing that action as 'the' only correct answer.

- Creates a shared, intersubjective vocabulary of action through the taxonomy and graph view search
- Provides a variety of ways of deriving and combining document and user meta-data.

Guidance Consulted: Recognising Relevant Collaborators

How will access be modulated to account for different information needs?

How can one ensure that all relevant stakeholders are invited to participate either right from the beginning or at a later stage?

CISs should not just support people in noticing other documents, but also new stakeholders and counterparts in other regions, especially those that have not been previously engaged with but could be of great value in collaborations or help achieve a goal.

- Author information for related documents within the search results contains contact information. Clicking on the author's name will provide an email address, internal to the system, through which searchers can initiate contact with authors (Figure 16).

Details	Document	Topics
▲	CBRN National Action Plans	Lists of nuclear disasters and radioactive incidents, Action plan, SARS, Centres of Excellence
<div><div>CBRN National Action Plans Chemical Biological Radiological Nuclear Risk Mitigation - Centres of Excellence Jointly implemented by the EC JRC and UNICRI CBRN National Action Plans Senior Strategy and Policy Advisor UNICRI Status of the Regional Secretariats Manila</div><div><p>Topics:</p><ol style="list-style-type: none">1. Lists of nuclear disasters and radioactive incidents2. Action plan3. SARS4. Centres of Excellence</div><div><p>Author: Torben Sauerland Source: filesystem Date: 2014-05-12 Country: United Kingdom Graph Edit</p></div></div>		

Figure 16 Knowledge Base entry details showing meta-data and author name (right hand side, top of list) that is an email link.

7.2.3 NEC/RescueRoam/Collaborative Platform

A range of interrelated communication and connectivity tools was designed for the users of SecInCoRe. They produce an ensemble of securely connection possibilities to a CIS from anywhere. The Rescue Roam provides a single-sign-on and wifi connectivity for users, making it possible both for local networks to be set up and for users to rely on the same credentials to access their CIS from wherever they are. The NEC and the Collaborative Platform are two ways in which secure, self-selected, group communication can take place. Such tools that support system **accessibility** and **cooperation** need to also have clear practices of **accountability**, **privacy**, **data protection**, and **information self-determination** as their users create traceable accounts and have the ability to see and find each other.

Guidance Consulted: Protecting the Rights of Data Subjects

How are data subjects informed of their rights from the management/host perspective?

What about the rights of the users whose data is being logged?

In order to comply with the EU's General Data Protection Regulation, which focuses on user ownership of their data, any communication system needs to make what is tracked transparent to a user so they can exercise their right to request it be corrected or deleted. Users need to be not just made aware that data is being kept, even if the public version is anonymised, but consent to how it is being processed.

- The entry page to these tools on the demonstrator offers direct links to ELSI guidance (Privacy and Personal Data Protection, Transparency of Data Protection) that support users in understanding their rights and engaging critically with how the different data gathered by these systems are combined.
- The entry page to these tools on the demonstrator offers direct links to ELSI guidance (e.g. Protecting the rights of Data Subjects, Data Controllers, Data Protection Impact Assessments) that support hosts and managers in understanding and enacting their responsibility towards data protection regulations towards such things like developing making clear to users what data is stored and how consent it tracked.

Guidance Consulted: Justifying Exclusion

CISs, while aiming to support collaboration, also need provide the potential to restrict and limit interactions in ways that do not technologically inscribe discrimination and injustice. Doing so can help balance trust in the technology with trust in collaborators. In other words, trust and security sometimes come from not sharing everything with everyone and maintaining control, while at other times restrictions and exclusions decrease trust and security.

- The NEC and collaborative platform both allow for the ability to connect to self-selected individuals and groups with the ability to add in new users or remove old users without losing connectivity (Figure 17).
- The overall system provides multiple alternative channels of interaction, where communication groups can take different members and forms.



Figure 17 The QR codes that enable the self-selected communication groups within the NEC



8 Wider Societal Implications and Future Work

Many proclaim that the nature of emergencies is changing in a globalised “new world” which is characterised by an ‘ever increasing interrelatedness and interdependence’ (Boin & Ekengren, 2009). Along similar lines, social theorists and technology scholars talk about new forms of transboundary risks and crises that can quickly spread across geographical borders and policy boundaries (Ansell *et al*, 2010; Lagadec, 2009; Rosenthal, 2003). With these new forms of risk, decision-making for disaster risk management needs to accommodate the possibility to negotiate different interests, forms of knowledge, and ways of qualifying authority. This requires accepting that conflicting views may be inherent to the process of good disaster risk management (see Storni 2013, DiSalvo 2010).

This is especially the case when dealing with ethical, legal, and social issues around DRM. Ethical values are relative, situated, and contextual. In many European societies, ethics has become pluralized and ethical values change over time, and thus become objects of negotiation and intermediation. They are, and should be, the subject of open democratic debate (Habermas, 1994; Habermas, 1996; Mouffe, 2000; Rawls, 1971).

ELSI as a framework was developed as a way to reconcile ethics, society, and the technosciences. Too often it has been translated into a need to seek ‘acceptance’, conduct ‘assessments’ as a way of ‘policing’ design or even at the end of design to ‘approve’ design. This approach separates ethical, legal and social ‘Issues’ from the social, material, technical contexts in which they emerge and constructs agency as locatable in humans only. However, ethics, lawfulness, and social responsibility arise in the ‘intra-actions’ of the many elements involved making it difficult, if not impossible, to isolate the human, the technological, the organisational or regulatory. There have always been tensions (Viseu 2015) and now there are calls for the development of a post-ELSI framework (Balmer *et al* 2016).

However, for such debates to happen, ELSI have to be noticed and turn from matters of fact, that is, accepted, unnoticed, taken for granted, common-sense facts of life, into ‘matters of concern’, that is, interrogated, dissected, contested objects of critique (Latour, 2005). The ELSI Guidance draws its form from these needs and supports the necessary processes of noticing and debating.

8.1 *Some comments about current societal tensions affecting this guidance*

8.1.1 Revisiting European Values

A starting point for this ELSI work has been core European values, enshrined in the European Convention on Human Rights, including respect for human dignity, liberty, democracy, equality, and the rule of law. Current global dynamics put these values under the test.

These values have always been based on inherent contradictions between a universal and Eurocentric ideal and the exclusion of “peripheral others” who do not fit into this image. They also stand in tension between the rights of an individual and the rights of a community (both local and international) (McInerney-Lankford 2011). These tensions are currently amplified by the ongoing refugee/migrant crisis on the one hand, and the struggles to reconfirm the freedom of movement of (some) people as a founding principle of the EU, on the other; a tension mapped out in the fluidity of categorisations as European citizens working in the UK and UK citizens living in Europe, who had conceived of themselves as European citizens free to move, become migrants.



Confronted with these complexities, it is not enough to merely repeat a commitment to EU values as fixed and abstract ideals. What is needed is to critically, creatively, and actively work towards new expressions of these values that can engage with the complexity but also situatedness of societal necessities, social possibilities, and technological innovation. Braidotti (2006, 2013), for example, urges us to imagine a new political and ethical European project which firmly resists the current forces that envision security in such a way that pushes us towards 'Fortress Europe' and instead she argues for reviving tolerance as a tool of social justice (see also Brown 2006). Such a visionary project is based on an affirmative politics which combines critique – that is the ability to see opportunities in challenges and differences rather than just limitations – with creativity that urges us to imagine afresh opportunities that are offered amidst this unsettling of values, ideals and fixed references.

That is why we take our approach of not just evaluating the ethical and social effects and implications of technologies as an after-design-time event but participating in creating and designing technologies in ethically circumspect ways.

8.1.2 From unity and solidarity to contested democratic engagements

Europe's current levels of peace and stability are unprecedented within its history. However, in an era where globalization and nationalism are at loggerheads, the complexities and challenges facing the EU are considerable. Security threats and challenges, too, are becoming 'more diverse, less visible and less predictable' (European Commission, 2003) while current events such as the always looming Grexit and the now decided Brexit are further evidence of the tensions with which Europe's prosperity, future, and humanitarian values stand. Challenges such as extreme weather and climate change, the refugee/migration crisis, terrorism threats, organised crime and other environmental or social disasters highlight vulnerabilities as well as the simultaneously local and global character of risks.

Being the political and economic union of currently 28 member states, the European Union has been trying to respond to these complex crises by striking a balance between increasing transnational cooperation and solidarity while respecting the sovereignty and subsidiarity of its member states; a strategy that is reflected in its motto "united through diversity" (European Communities 2015). However, it is far from clear how this precarious balance can be achieved. While some call for further convergence, or for a 'new security paradigm' which will see the European Union assume a supranational and newly emerging security role (Boin and Ekengren 2009), others point to the very diverse institutional and cultural traditions and strategies that shape crisis and disaster management within member states or even within regions (Bremberg and Britz, 2009; Bossong and Hegemann 2015).

These efforts have resulted in an ambivalent mix of policies and institutions. For example, within the EU so called "macro-regions" are emerging, partly prompted by security concerns, such as the [EUSDR](#) (EU Strategy for the Danube Region) and [EUSBSR](#) (EU Strategy for the Baltic Sea Region). Such initiatives may lead to increased coordination and enhanced efficiency within a region, but may also, in the long-term, result in the fragmentation of the EU framework as new boundaries accumulate, duplicate effort, and clash (Olsson 2009).

Similar effects may also result in DRM at the EU level, as such forms of 'unity' may duplicate and clash with existing bilateral or regional or international agreements or arrangements which have been established within the UN (BRIDGE 12.2). While these attempts are initiated as the result of desires for greater security over a region, fragmentation often leads to institutionalised silos and can actually decrease security by undermining trust across boundaries and borders.



This guidance can help address such challenges by approaching collaboration, coordination, and interoperability in ways that do not rely on a basis of consensus. Consensus, in fact, can be undesirable when seeking to build truly democratic spaces (Jasanoff cited in Callon et al 2009). Instead of seeking unity that finds commonalities and spaces of agreement, democracy also requires “agonistic pluralism”.

What is specific and valuable about modern liberal democracy is that, when properly understood, it creates a space in which this confrontation is kept open, power relations are always being put into question and no victory can be final. However, such an ‘agonistic’ democracy requires accepting that conflict and division are inherent to politics and that there is no place where reconciliation could be definitively achieved as the full actualization of the unity of ‘the people’. (Mouffe 2000, p. 15, see also DiSalvo 2010)

The ELSI Guidance platform envisions such a space. Using reflexive questions it allows contestation and invites differing understandings. Instead of attempting to provide fixed, and hence always inadequate, answers, it prompts reflection and debating. And instead of seeking to locate the common denominator of consensus -- which ignores differing voices and experiences -- it seeks to bring forth the potential for growth and for innovative solutions that arise from engaging with, rather than just bridging between, diversity.

8.1.3 New media and new publics

New and emerging information and communication technologies have the ability to transform disaster risk management practices in unique ways as they act as sources of data, become tools for analysis, and engender new public and professional expectations of disaster response and responsibility (D2.6). In doing so, they have created diverse new ‘publics’ which demand a voice in social, political and environmental decisions.

The idea of publics, plural, brings the focus on the diverse, overlapping, yet clashing ways in which individuals, communities, and citizens can be classified and organised for understanding. Often this is by class, vulnerability, risk, etc. However, the latest political events of Brexit, the controversial election of Donald Trump as the President of the US, and the new representation in the upcoming French Election have starkly demonstrated the potential strength of the voices of new publics and the consequences for trust, solidarity, and the ability to create “unity in diversity” if not meaningfully engaging with them. At the same time, the growing uncertainties and frequency of disasters have led disaster risk management to look for wider collaboration between diverse stakeholders encompassing federal, state and local levels of government, as well as private businesses, voluntary organisations, and most pertinently, communities and citizens themselves. It is at this juncture that the questions of how *should* these diverse stakeholders interact become extremely pertinent (Buscher et al 2017).

This Guidance focuses on how to engage with DRM in a way that envisages engagement of different actors as complementary to formal efforts and shows that risk governance requires not only expert professionalism and broad-based engagement with local knowledge, but also an understanding of how vulnerability and resilience reflect and enact political choices that affect individuals and communities unequally (Jasanoff 2010; for further discussion, see Büscher et al 2017, in press).



8.1.4 Implications

These new forms of social interaction require technology that can work beyond traditional command and control models of DRM, as the hierarchical divisions of responsibility and vertical lines of communication in this model hamper locally flexible management and diminish the emergency services' capability to activate community resilience (Birkland, 2009, p.430). Furthermore, innovation in mobile and broadband communications networks, cloud computing, and common information space concepts, such as that pursued by EU project -- such as SecInCoRe, EPISECC, SECTOR, REDIRNET -- have the potential to engage novel ways of working with and sharing information. These technologies raise new risks and challenges, as well as new opportunities.

The challenge moves from how to achieve unity through diversity to the question how to achieve *cooperation/collaboration* through contestation and conflict. And it is exacerbated by the fact that these types of ELSI cannot be solved by focused on the social or political, but equally require attention to the technological, environmental, and material (Latour 2005).

The ELSI Guidance community platform described in this document opens up the space for deliberation to include the very technologies that are developed and adopted to pursue these goals. Such a new project is based on values that are live (actively present to support and strengthen its people), lived (conscious and clear of its situatedness, and its cultural and political positionings) and living (open to debate and change), and our ELSI work is foundation work towards this. This is not just about making analytical points but about rethinking the normative, such as what responsibility, diversity, resilience mean in such a complex world. But also about creating the infrastructures that enable this rethinking to take place.



9 Future Work

The work presented here is the result of a collaborative effort led by Monika Büscher and Katrina Petersen at Lancaster University, developing contributions from the SecInCoRe, EPISECC, SECTOR, REDIRNET projects predominantly, but also incorporating contributions from the BRIDGE, ConCORDe and IMPRESS projects as well as contributions from many practitioner and developer participants in our workshops. Over the course of 2016, this collaboration has been extended to include the Public Safety Communications Europe Network (PSCE), who has agreed to host the ELSI Guidance as a community platform beyond the ends of the projects involved. In this section we describe some core aspects of future work planned.

9.1 Plans

The long-term goal of the collaboration is to develop a research-based service for responsible research and innovation (RRI) in DRM, building out from the existing ELSI Guidance. Working backwards, the steps towards this include

2019 - 2024 **'AttentoRRI'- Pro-Active responsible research and innovation in disaster risk management'** developing the content, methods, networks, governance structures and business models needed for the RRI in DRM Service

2018 A 1 year CSA **RRI in DRM - Best Practice** to develop ELSI Guidance. The aims are:

- To develop **Research Ethics Guidance** for EU RRI
- To **extend ELSI Guidance**, explore how other dimensions than CIS, such as 4/5G, wearables, machine learning, MPC, etc. could be supported
- Construct an Inventory of examples of **'Best Practice in Design and Use'**

2017 May 2017: Launch of www.islTethical.eu at the PSCE Conference

By 28 April 2017, the platform will be functioning prototype fit for public engagement. It is a prototype in the sense of aspects of its functionalities and content are under development.

- it will have working content, links, a search function, a contributors' corner that enables contribution of examples, principles, guidance as well as comments.
- the site will include an open description of the governance for the platform.
- the site will include a mechanism to monitor contributions made through the contributors' corner.
- An ELSI Whitepaper will be available on the PSCE website to explain the background of the platform, which will link to this Deliverable.

In addition to developing the ELSI Guidance Community Platform, ULANC have led ELSI Task Force efforts to enable the incorporation of ELSI terms into the CEN Workshop Agreement on Terminologies in Crisis and Disasters. This is ongoing.



9.2 Memorandum of Understanding

Below is the Memorandum of understanding signed between PSCE and the Centre for Mobilities Research and Lancaster University to govern, maintain, and grown the ELSI Guidance and isitethical.eu platform (Figure 18).

Memorandum of understanding

This "Memorandum of Understanding" is agreed between the Public Safety Communications Europe Network (PSCE) represented by their Secretary; the Centre for Mobilities Research at Lancaster University (Cemore), represented by their Director

After 28 April 2017, PSCE agrees to host the ELSI Guidance at isitethical.eu and will observe the following:


- The site will be maintained to the minimum of the functioning prototype released in May 2017 by PSCE in dialog with the director of Cemore. In case of disagreements, a consensus will be sought.
- PSCE will promptly (within three weeks) implement any changes requested by the director of Cemore
- PSCE will promote the platform amongst its members
- PSCE will provide feedback to the Cemore Director

Cemore support the ELSI Guidance platform beyond the end of the SecInCoRe project and will observe the following:

Cemore support the ELSI Guidance platform beyond the end of the SecInCoRe project and will observe the following:

- Monika Büscher and Catherine Easton will monitor contributions on an at least bi-monthly basis, on or nearest the 30th of every other month
- Where possible, Monika Büscher and Catherine Easton will promptly (within three weeks) address any issues raised by PSCE, as well as seek to amend content or provide new content as possible
- Monika Büscher and Catherine Easton and relevant Cemore members will promote the platform amongst its members
- Cemore will seek funding for further development

If a different action from those previewed in this Memorandum regarding the governance of the platform will have to take place, it has to be previously agreed upon between PSCE and Cemore.



SIGNED Marie-Christine Bonnamour, Secretary General DATE 22/03/2017 for PSCE

SIGNED Monika Büscher DATE 5 April 2017 Cemore

Figure 18 A copy of the signed MOU



9.3 *ELSI Guidance Governance*

The Current Editors of the Guidance are Monika Büscher, Catherine Easton, Katrina Petersen, Xaroula Kerasidou.

Contributors include: Andreas Baur-Ahrens, Sarah Becklake, Lina Jasmontaite, Kristof Huysmans, Matthias Leese, Toni Staykova, TBC\$

Collaborating contributors include: David Lund, Marie-Christine Bonnamour, George Mourikas

The Guidance is available under a Creative Commons Licence – People are Free to use and amend, provided credit is given.

Membership in the community platform is open to anyone. People have to sign up with the real names and addresses. They can choose a pseudonym, and choose to have their information locked.

Anyone can contribute examples, candidate guidance, principles, and comments. All contributions are monitored and it may take up to two months before they are approved.

PSCE and Cemore are in dialog over the content. Changes are tracked and discussed at regular review meetings (bi-annual).

9.4 *Further Research Required*

There are many approaches to addressing ELSI in the field of DRM research and innovation. ELSI are particularly challenging and significant in this domain, because of the exceptional nature of disasters and the exceptional demands these make on people, technologies, and regulatory frameworks. Current research efforts are often siloed within individual projects, which leads to inconsistent approaches, practices that ‘reinvent the wheel’, a failure to share best practice, and persistence of suboptimal practices, much uncertainty and disorientation. This slows innovation down and - most importantly - produces innovations that do not make the most of existing knowledge or existing ‘solutions’. There are a few initiatives that cut across different projects, for example the standardisation of Ethical Impact Assessment led by the SATORI consortium or our own efforts to develop ELSI Guidance for using and governing common information spaces in disaster risk management, which has brought together a wide range of projects .

The results to date from these cross-cutting efforts suggest that significant competitive edge can be gained from seriously ELSI reflexive innovation. To strengthen this work, research on the different dimensions of how ELSI can be engaged with as part of design and what ELSI emerge consistently in a range of collaborative disaster IT settings is needed.

It would be helpful to develop practical **Research Ethics Guidance** for EU RRI to the platform. This should give sample participant information sheets and informed consent forms, open research ethics protocols, a best practice inventory of cases of gaining approval from relevant authorities, a database with contacts. This requires research into the relevant authorities and the requirements they make.

This should be complemented by more conceptual and methodologically wide-ranging research on theories and methods of responsible research and innovation and their particular role in innovation for DRM.

An integral part of this research should be an ambition to **extend the ELSI Guidance**, for example to explore how other dimensions than CIS, such as 4/5G, wearables, sensors, machine learning, Multi Party Computing, etc. could be supported.

To support ways of making ELSI Guidance ‘live’, it would be very useful to have a living **inventory of ongoing research and socio-technical innovation in relation to ELSI**. To



make it 'lived', research on **best practice** is needed, and to make this a 'living' resource, we need further research on facilitating community engagement in essentially 'crowd-sourcing' insight into complex challenges such as ELSI.

Research on methodological innovation in developing interdisciplinary creative EIA approaches that fold insights into pro-active socio-technical innovation.

Research on governance and business models for collaborative ICT in DRM is needed.

As a result of this research, a broader and deeper version of the ELSI Guidance could be developed, including a chapter on research ethics. The content would support more consistent and higher quality research ethics and ELSI-proactive innovation. This Guidance would move towards standardisation through extensive stakeholder engagement from the 'needs' end of DRM.

This future research is needed to engender better ethical, social, and legal reflexivity in innovation for disaster risk management. By developing 'standard' guidance based on broad collaboration with stakeholders for proactive and critical assessment of ELSI arising in ICT for DRM that acknowledges the situationally-relevant nature of these challenges and opportunities, the potential of new technologies might be leveraged more radically and carefully, and challenges and risks could be mitigated.



10 Literature Index

- ALLEA (2017) *The European Code of Conduct for Research Integrity*, Revised Edition. All European Academies. <http://www.allea.org/wp-content/uploads/2017/03/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017-1.pdf>
- Ansell, C., Boin, A., & Keller, A. (2010) Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System. *Journal of Contingencies and Crisis Management*, 18: 195-207.
- Carroll, J. M. (2000) Five reasons for scenario-based design. *Interacting with Computers*, 13: 43–60.
- Balka, E. (2006) Inside the Belly of the Beast: The Challenges and Successes of a Reformist Participatory Agenda. *Proceedings of the ninth Participatory Design Conference*. 134-143.
- Balmer, A. S., Calvert, J., Marris, C., Molyneux-Hodgson, S., Frow, E., Kearnes, M., Bulpin, K., Schyfter, P., Mackenzie, A. & Martin, P. (2016) Five Rules of Thumb for Post-ELSI Interdisciplinary Collaborations, *Journal of Responsible Innovation*, DOI: 10.1080/23299460.2016.1177867
- Benkler, Y., Shaw, A., & Hill, B. M. (2013). Peer Production: A Modality of Collective Intelligence. In M. Bernstein & T. Malone (eds.), *Collective Intelligence*. Retrieved from http://mako.cc/academic/benkler_shaw_hill-peer_production_ci.pdf [Accessed 4th April 2014]
- Bodker, S. (2000) Scenarios in user-centred design--setting the stage for reflection and action. *Interacting with Computers*, 13: 61–75.
- Boin, A., & Ekengren, M. (2009). Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union. *Journal of Contingencies and Crisis Management*, 17: 285-94.
- Bogost, I. (2007). *Persuasive games: The expressive power of videogames*. MIT Press.
- Braidotti, R., 2013. *The Posthuman*. Cambridge: Polity.
- Braidotti, R., 2006. The becoming-minoritarian of Europe. *Deleuze and the Contemporary World*, 79.
- Brey, P. (2000) Disclosive Computer Ethics. *Computers and Society*, 30, 4, 10–16.
- Buchanan, R. (1985). Declaration by design: Rhetoric, argument, and demonstration in design practice. *Design Issues*, 4-22.
- Büscher, M., Liegl, M., Perng, S., Wood, L. (2014) How to Follow the Information? *Sociologica*. 1, Doi: 10.2383/77044
- Büscher, M., Liegl, M., Rizza, C. & Watson, H. (2014) How to do IT more carefully? Ethical, Legal and Social Issues (ELSI) in IT Supported Crisis Response and Management. *International Journal of Information Systems for Crisis Response and Management*, 6 (4): iv-xxiii.
- Büscher, M., Liegl, M., & Wahlgren, P. (2013) *D12.2 BRIDGE Ethical, Legal and Social Issues: Current practices in Multi Agency Emergency Collaboration*. Available at http://www.bridgeproject.eu/downloads/d12.2_bridge_elsi.pdf
- Callon, M. Lascoumes, P. & Barther, Y. (2009) *Acting in an uncertain world, an essay on technical democracy*, Cambridge: MIT Press.



- Cavoukian, A. (2001) *Taking Care of Business: Privacy by Design*. Presentation given at the IBM/Tivoli Privacy Summit, 31 May, Toronto. Available at: <http://www.ontla.on.ca/library/repository/mon/2000/10296375.pdf>
- Chesbrough, H. W. (2003) *Open Innovation: The New Imperative for Creating and Profiting from Technology*. Boston: Harvard Business School Press.
- Clarke, K., Hardstone, G., Rouncefield, M., & Sommerville, I. (2006) *Trust in Technology: A Socio-Technical Perspective*. London: Springer.
- Coulton, P., Burnett, D., & Gradinar, A. I. (2016) Games as speculative design: allowing players to consider alternate presents and plausible futures. In P. Lloyd, & E. Bohemia (eds.), *Proceedings of Design Research Society Conference 2016*: 1609-1626).
- DiSalvo, C. (2010) Design, democracy and agonistic pluralism, *Proceedings of the Research Design Society Conference*, 7-9 July 2010. Montreal (Quebec), Canada: Université de Montréal.
- DiSalvo, C., Lodato, T., Jenkins, T., Lukens, J., & Kim, T. (2014) Making public things: how HCI design can express matters of concern. *Chi 2014*: 2397–2406. <http://doi.org/10.1145/2556288.2557359>
- Dratwa, J. (ed.). (2014). *Ethics of Security and Surveillance Technologies* (Opinion no, pp. 1–165). Brussels: European Group on Ethics in Science and New Technologies to the European Commission.
- Dunne, A. (2008). *Hertzian tales: Electronic products, aesthetic experience, and critical design*. Cambridge, MA: MIT Press.
- European Commission (2013). *Risk-Benefit Analyses and Ethical Issues: A guidance document for researchers complying with requests from the European Commission Ethics Reviews*. Luxembourg: Publications Office of the European Union.
- European Communities (2005). Treaty Establishing a Constitution for Europe (2005). Available at: http://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_en.pdf
- FET Advisory Group (2016) The need to integrate the Social Sciences and Humanities with Science and Engineering in Horizon 2020 and beyond. Available at: <https://ec.europa.eu/programmes/horizon2020/en/news/report-need-integrate-social-sciences-and-humanities-science-and-engineering-horizon-2020>
- Flanagan, M. (2009) *Critical play: radical game design*. Cambridge, MA: MIT press.
- Frayling, C. (1994) Research in art and design. *Royal College of Art*, 1 (1): 1-5.
- Friedman, B., Kahn Jr, P. H., & Borning, A. (2013) Value Sensitive Design and Information Systems. In N. Doorn, D. Schuurbijs, I. van de Poel, and M. Gorman (eds.), *Early Engagement and New Technologies: Opening up the Laboratory*. London: Springer, 55–95.
- Geertz, C. (1973) *The Interpretation of Culture*. New York: Basic Books.
- Habermas, J. (1994) *Postmetaphysical Thinking: Philosophical Essays*. Cambridge: MIT Press.
- Habermas, J. (1996) *Between facts and norms: contributions to a discourse theory of law and democracy* Cambridge: MIT Press.



- HM Government (2013) *Emergency Response and Recovery Non statutory guidance accompanying the Civil Contingencies Act 2004*. Cabinet Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/253488/Emergency_Response_and_Recovery_5th_edition_October_2013.pdf
- Hollnagel, E., & Woods, D. D. (2005) *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*. Boca Raton: CRC Press. doi:10.1201/9781420038194
- Jasanoff, S. (2010) Beyond Calculation: A Democratic Response to Risk, In G. Lakoff (ed.), *Disaster and the Politics of Intervention*. New York: Columbia University Press, 14-41.
- Lagadec, P. (2009) A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice. *Review of Policy Research*, 26: 473-86.
- Lash, S., & Urry, J. (1994) *Economies of Signs and Space*. London: Sage.
- Latour, B. (2005) From Realpolitik to Dingpolitik or How to Make Things Public. In B. Latour & P. Weibel (eds.), *Making Things Public-Atmospheres of Democracy*. Cambridge, MA: MIT Press, 1–31.
- Law, J., & Urry, J. (2004) Enacting the social. *Economy and society*, 33(3), 390-410.
- Letouzé, E., Meier, P., & Vinck, P. (2013) Big Data for Conflict Prevention: New Oil and Old Fires. In F. Mancini (ed.), *New Technology and the Prevention of Violence and Conflict* (pp. 4–27). New York: International Peace Institute.
- Lévy, P. (1997) *Collective Intelligence. Mankind's Emerging World in Cyberspace*. Translated by R. Bononno. Cambridge, MA: Perseus Books.
- Lury, C., & Wakeford, N. (eds.). (2012) *Inventive methods: The happening of the social*. Routledge.
- McInerney-Lankford, S., Darrow, M., & Rajamani, L. (2011) *Human Rights and Climate Change: A review of the international legal dimensions*. A World Bank Study. Doc. 61308. Available at: <http://siteresources.worldbank.org/INTLAWJUSTICE/Resources/HumanRightsAndClimateChange.pdf>
- Michael, M. (2009) Publics performing publics: of PiGs, PiPs and politics. *Public Understanding of Science*, 18(5): 617-631.
- Montavani, G. (2000) *Exploring Borders: Understanding Culture and Psychology*. London: Routledge.
- Mouffe, C. (2000) *The Democratic Paradox*. New York: Verso.
- Nissenbaum, H. (1998) Values in the design of computer systems. *Computers in Society*, 28 (1): 38–39.
- Olsson, S. (ed.) (2009) *Crisis Management in the European Union: Cooperation the Face of Emergencies*. Springer: Dordrech, 8-9.
- Palen, L., Vieweg, S., Sutton, J., & Liu, S. B. (2009) Crisis Informatics: Studying Crisis in a Networked World. *Social Science Computer Review*, 27(4): 467–480. doi:10.1177/0894439309332302
- Palen, L., Vieweg, S., Sutton, J., & Liu, S. B. (2009) Crisis Informatics: Studying Crisis in a Networked World. *Social Science Computer Review*, 27, (4): 467–480.
- Pauwels, E. (2007) *Ethics for researchers*. Brussels: European Commission.



- Petersen, K., Oliphant, R., & Buscher, M. (2016) Experimenting with the Ethical Impact Assessment as a Grounding Socio-Technical Practice. *Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016*.
http://idl.iscram.org/files/katrinapetersen/2016/1364_KatrinaPetersen_etal2016.pdf
- Phillips, A. (2012) List. In C. Lury and N. Wakeford (eds) *Inventive Methods: The Happening of the Social*, New York: Routledge, 96-109.
- Pottebaum, J., Kuhnert, M., Schäfer, C., Behnke, D., Büscher, M., Petersen, K. & Wietfeld, C. (2016) Common Information Space for Collaborative Emergency Management. In *Proceedings of the IEEE International Symposium on Technologies for Homeland Security 2016, Boston*.
- Prieur, M. (2009) Ethical Principles on Disaster Risk Reduction and People's Resilience.
http://www.coe.int/t/dg4/majorhazards/ressources/pub/Ethical-Principles-Publication_EN.pdf
- Rawls, J. (1971) *A Theory of Justice*. London: Harvard University Press.
- Rogerson, S. (2009) Landscapes of ethical issues of emerging ICT applications in Europe. *Communication*. Retrieved from <http://hdl.handle.net/2086/2475>
- Rosenthal, U. (2003) September 11: Public Administration and the Study of Crises and Crisis Management. *Administration and Society*, 35: 129-43.
- Salem, F. & Jarrar, Y. (2010) Government 2.0? Technology, Trust and Collaboration in the UAE Public Sector. *Policy & Internet*, 2: 63-97.
- Salen, K., & Zimmerman, E. (2004) *Rules of play: Game design fundamentals*. Cambridge: MIT press.
- Schot, J., and Rip, A. (1997) The past and future of constructive technology assessment. *Technological Forecasting and Social Change*, 54 (2-3): 251–268.
doi:10.1016/S0040-1625(96)00180-1
- Storni, C. (2013) Design for future uses: Pluralism, fetishism and ignorance. Proceedings of the [Nordic Design Research Conference 2013: Experiments in design research](#). Copenhagen, Denmark and Malmö, Sweden, June 9-12.
- Thrift, N. (2005) *Knowing Capitalism*. London: Sage.
- Thrift, N. (2011) Lifeworld Inc—and what to do about it. *Environment and Planning. D, Society & Space*, 29(1), 5–26. doi:10.1068/d0310
- UNESCO (2014) *From Words to Action*. The United Nations Educational, Scientific and Cultural Organization. Available at:
<http://unesdoc.unesco.org/images/0023/002311/231132m.pdf>
- UNISDR. (2015) *Sendai Framework for Disaster Risk Reduction - UNISDR*. Retrieved from <http://www.unisdr.org/we/coordinate/sendai-framework>
- Verbeek, P.-P. (2011) *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago: University of Chicago Press.
- Viseu, A. (2015) Integration of social science into research is crucial. *Nature*, 525: 291.
- Von Schomberg, R. (2013) A vision of responsible innovation. In R. Owen, J. Bessant, & M. Heintz (eds.), *Responsible innovation*. London: Wiley, 51–74.
doi:10.1002/9781118551424.ch3



- Wright, D. (2011) A framework for the ethical impact assessment of information technology. *Ethics and Information Technology*, 13 (3): 199–226. <http://doi.org/10.1007/s10676-010-9242-6>
- Yoo, D., Hultgren, A., Woelfer, J. P., Hendry, D. G., & Friedman, B. (2013) A value sensitive action-reflection model. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. New York: ACM Press, 419-428.
- Zilgalvis, P. (2009) *Ethics and Governance in the 7th framework programme*. Retrieved from: http://ec.europa.eu/research/conferences/2009/rtd-2009/presentations/ethics/p_zilgalvis___ethics_and_governance_in_the_7th_framework_programme.pdf